МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФГБОУ ВО «Уральский государственный экономический университет»

Одобрена
на заседании кафедры

27.11.2025 г.

протокол № 3

Зав. кафедрой Карпов А.Е.

Утверждена
Советом по учебно-методическим вопросам и качеству образования

16 декабря 2025 г.

протокол № 4

Председатель _____ Карх Д.А.
(подпись)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование дисциплины	Информационная безопасность телекоммуникационных систем
Направление подготовки	02.03.03 Математическое обеспечение и администрирование информационных систем
Профиль	Прикладной искусственный интеллект
Форма обучения	очная
Год набора	2026

Разработана:
Профессор, д.т.н.
Часовских В.П.

Доцент, к.ф.-м.н.
Филиппов С.Д.

Екатеринбург
2025 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Рабочая программа дисциплины является частью основной профессиональной образовательной программы высшего образования - программы бакалавриата, разработанной в соответствии с ФГОС ВО

ФГОС ВО	Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 02.03.03 Математическое обеспечение и администрирование информационных систем (приказ Минобрнауки России от 23.08.2017 г. № 809)

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

раскрытие сущности информационной безопасности и защиты информации, определение теоретических, методологических и организационных основ обеспечения безопасности информации, ознакомление с тенденцией развития информационной безопасности, с моделями возможных угроз, терминологией и основными понятиями теории безопасности информации

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина относится к части, формируемой участниками образовательных отношений.

3. ОБЪЕМ ДИСЦИПЛИНЫ

Промежуточная аттестация	Часов					З.е.
	Всего за семестр	Контактная работа .(по уч.зан.)			Самостоятельная работа в том числе подготовка контрольных и курсовых	
		Всего	Лекции	Лабораторные		
Семестр 5						
Зачет	108	48	24	24	60	3
Семестр 6						
Экзамен	144	32	0	32	85	4
	252	80	24	56	145	7

4.ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ОПОП

В результате освоения ОПОП у выпускника должны быть сформированы компетенции, установленные в соответствии ФГОС ВО.

Шифр и наименование компетенции	Индикаторы достижения компетенций
производственно-технологический	

ПК-3 Разработка архитектуры ИС в рамках выполнения работ и управления работами по созданию (модификации) и сопровождению ИС	ИД-1.ПК-3 Знать: инструменты и методы проектирования архитектуры ИС; инструменты и методы верификации архитектуры ИС; возможности ИС; предметную область автоматизации; архитектуру, устройство и функционирование вычислительных систем; коммуникационное оборудование; сетевые протоколы; основы современных операционных систем; основы современных СУБД; устройство и функционирование современных ИС; архитектуру мультиарендного программного обеспечения; основы ИБ организации; современные стандарты информационного взаимодействия систем; программные средства и платформы инфраструктуры информационных технологий организаций; современные подходы и стандарты автоматизации организации; системы классификации и кодирования информации, в том числе присвоения кодов документам и элементам справочников; отраслевую нормативно-техническую документацию; источники информации, необходимой для профессиональной деятельности при выполнении работ и управлении работами по созданию (модификации) и сопровождению ИС; лучшие практики создания (модификации) и сопровождения ИС в экономике; основы бухгалтерского учета и отчетности организаций; основы налогового законодательства Российской Федерации; основы управленческого учета; основы международных стандартов финансовой отчетности; основы управления торговлей, поставками и запасами; основы организации производства; основы управления персоналом, включая вопросы оплаты труда; основы финансового учета и бюджетирования; основы управления взаимоотношениями с клиентами и заказчиками; современные инструменты и методы управления организацией, в том числе методы планирования деятельности, распределения поручений, контроля исполнения, принятия решений; методологию ведения документооборота в организациях; инструменты и методы определения финансовых и производственных показателей деятельности организаций; культуру речи; правила деловой переписки.

ПК-3 Разработка архитектуры ИС в рамках выполнения работ и управления работами по созданию (модификации) и сопровождению ИС	ИД-2.ПК-3 Уметь: проектировать архитектуру ИС в рамках выполнения работ и управления работами по созданию (модификации) и сопровождению ИС; проверять (верифицировать) архитектуру ИС в рамках выполнения работ и управления работами по созданию (модификации) и сопровождению ИС; анализировать исходную документацию в рамках выполнения работ и управления работами по созданию (модификации) и сопровождению ИС; разрабатывать документы в рамках выполнения работ и управления работами по созданию (модификации) и сопровождению ИС; осуществлять коммуникации с заинтересованными сторонами в рамках выполнения работ и управления работами по созданию (модификации) и сопровождению ИС.
	ИД-3.ПК-3 Иметь практический опыт: создания вариантов архитектурных спецификаций ИС в рамках выполнения работ и управления работами по созданию (модификации) и сопровождению ИС; выбора и согласования с заинтересованными сторонами оптимальной архитектурной спецификации ИС в рамках выполнения работ и управления работами по созданию (модификации) и сопровождению ИС.

ПК-4 Разработка прототипов ИС в рамках выполнения работ и управления работами по созданию (модификации) и сопровождению ИС	ИД-1.ПК-4 Знать: языки программирования и работы с базами данных; инструменты и методы модульного тестирования; инструменты и методы тестирования нефункциональных и функциональных характеристик ИС; инструменты и методы прототипирования пользовательского интерфейса; возможности ИС; предметную область автоматизации; технологии межличностной и групповой коммуникации в деловом взаимодействии, основы конфликтологии; технологии подготовки и проведения презентаций; основы современных операционных систем; основы современных СУБД; устройство и функционирование современных ИС; архитектуру мультиарендного программного обеспечения; основы ИБ организации; теорию баз данных; системы хранения и анализа баз данных; основы программирования; современные объектно-ориентированные языки программирования; современные структурные языки программирования; языки современных бизнес-приложений; современные методики тестирования разрабатываемых ИС; современные стандарты информационного взаимодействия систем; программные средства и платформы инфраструктуры информационных технологий организаций; современные подходы и стандарты автоматизации организации; системы классификации и кодирования информации, в том числе присвоения кодов документам и элементам справочников; отраслевую нормативно-техническую документацию; источники информации, необходимой для профессиональной деятельности при выполнении работ и управлении работами по созданию (модификации) и сопровождению ИС; лучшие практики создания (модификации) и сопровождения ИС в экономике; основы бухгалтерского учета и отчетности организаций; основы налогового законодательства Российской Федерации; основы финансового учета и бюджетирования; основы управленческого учета; основы международных стандартов финансовой отчетности; основы управления торговлей, поставками и запасами; основы организации производства; основы управления персоналом, включая вопросы оплаты труда; основы управления взаимоотношениями с клиентами и заказчиками; современные инструменты и методы управления организацией, в том числе методы планиро-вания деятельности, распределения поручений, контроля исполнения, принятия решений; методологию ведения документооборота в организациях; инструменты и методы определения финансовых и производственных показателей деятельности организаций; культуру речи; правила деловой переписки

ПК-4 Разработка прототипов ИС в рамках выполнения работ и управления работами по созданию (модификации) и сопровождению ИС	ИД-2.ПК-4 Уметь: кодировать на языках программирования в рамках выполнения работ и управления работами по созданию (модификации) и сопровождению ИС; тестировать результаты прототипирования ИС в рамках выполнения работ и управления работами по созданию (модификации) и сопровождению ИС; проводить презентации в рамках выполнения работ и управления работами по созданию (модификации) и сопровождению ИС; проводить переговоры в рамках выполнения работ и управления работами по созданию (модификации) и сопровождению ИС; работать с записями по качеству (в том числе с корректирующими действиями, предупрежда-ющими действиями, запросами на исправление несоответствий) в рамках выполнения работ и управления работами по созданию (модификации) и сопровождению ИС.
	ИД-3.ПК-4 Иметь практический опыт: разработки прототипа ИС в соответствии с требованиями заказчика к ИС в рамках выполнения работ и управления работами по созданию (модификации) и сопровождению ИС; тестирования прототипа ИС для проверки корректности архитектурных решений в рамках выполнения работ и управления работами по созданию (модификации) и сопровождению ИС; обработки результатов тестов прототипа ИС на корректность архитектурных решений в рамках выполнения работ и управления работами по созданию (модификации) и сопровождению ИС; принятия решения о пригодности архитектуры ИС в рамках выполнения работ и управления работами по созданию (модификации) и сопровождению ИС; согласования пользовательского интерфейса ИС с заказчиком ИС в рамках выполнения работ и управления работами по созданию (модификации) и сопровождению ИС; инициирования запросов на изменения (в том числе запросов на корректирующие действия, на предупреждающие действия, на исправление несоответствий) в рамках выполнения работ и управления работами по созданию (модификации) и сопровождению ИС.

5. ТЕМАТИЧЕСКИЙ ПЛАН

Тема	Часов						
	Наименование темы	Всего часов	Контактная работа .(по уч.зан.)			Самост. работа	Контроль самостоятельной работы
			Лекции	Лабораторные	Практические занятия		
Семестр 5		108					
Тема 1.	Основные понятия и анализ угроз информационной безопасности. Разработка политики информационной безопасности на уровне БД ((ПК-3, ПК-	8	2			6	

Тема 2.	Теоретические основы разработки автоматизированных средств (элементов) систем информационной безопасности. (ПК-3, ПК-4)	16	2	6		8	
Тема 3.	Классическая криптография (ПК-3, ПК-4)	12	2			10	
Тема 4.	Симметричные алгоритмы шифрования (ПК-3, ПК-4)	16	2	8		6	
Тема 5.	Хэш-функции (ПК-3, ПК-4)	18	2	10		6	
Тема 6.	Электронно-цифровая подпись (ПК-3, ПК-4)	8	2			6	
Тема 7.	Асимметричные алгоритмы шифрования (ПК-3, ПК-4)	8	2			6	
Тема 8.	Стеганография и стеганоанализ (ПК-3, ПК-4)	8	2			6	
Тема 9.	Уязвимости программного обеспечения (ПК-3, ПК-4)	8	2			6	
Тема 10.	Компьютерные вирусы и методы их обнаружения (ПК-3, ПК-4)	2	2				
Тема 11.	Разделение прав в операционных системах (ПК-3, ПК-4)	2	2				
Тема 12.	Методы авторизации и аутентификации пользователей (ПК-3, ПК-4)	1	1				
Тема 13.	Безопасность сетей ЭВМ (ПК-3, ПК-4)	1	1				
Семестр 6		117					
Тема 14.	Ассиметричные алгоритмы шифрования (продолжение) (ПК-3, ПК-4)	10		10			
Тема 15.	Стеганография и стеганоанализ (продолжение) (ПК-3, ПК-4)	10		10			
Тема 16.	Уязвимости программного обеспечения (продолжение) (ПК-3, ПК-4)	6		6			
Тема 17.	Компьютерные вирусы и методы их обнаружения (продолжение) (ПК-3, ПК-4)	30		6		24	
Тема 18.	Разделение прав в операционных системах (продолжение) (ПК-3, ПК-4)	20				20	
Тема 19.	Методы авторизации и аутентификации пользователей (продолжение) (ПК-3, ПК-4)	20				20	
Тема 20.	Безопасность сетей ЭВМ (продолжение) (ПК-3, ПК-4)	21				21	

6. ФОРМЫ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ШКАЛЫ ОЦЕНИВАНИЯ

Раздел/Тема	Вид оценочного средства	Описание оценочного средства	Критерии оценивания
Текущий контроль (Приложение 4)			

Темы 2	Тест №1 (Приложение 4)	Тест по вариантам из 3 задач	30 баллов: 10 баллов за каждую задачу
Темы 1, 7-12	Тест №2 (Приложение 4)	Тест из 30 вопросов	30 баллов: 1 балл за каждый вопрос
Темы 13 -20	Тест №3 (Приложение 4)	Тест из 60 вопросов	30 баллов: 1 балл за каждый вопрос
Промежуточная аттестация(Приложение 5)			
5 семестр (За)	Зачетные билеты (Приложение 5)	15 билетов, состоящих из 1 теоретического и 1 практического задания	70 баллов: 20 + 50 соответственно
6 семестр (Эк)	Экзаменационные билеты (Приложение 5)	15 билетов, состоящих из 1 теоретического и 1 практического задания	70 баллов: 20 + 50 соответственно

ОПИСАНИЕ ШКАЛ ОЦЕНИВАНИЯ

Показатель оценки освоения ОПОП формируется на основе объединения текущего контроля и промежуточной аттестации обучающегося.

Показатель рейтинга по каждой дисциплине выражается в процентах, который показывает уровень подготовки студента.

Текущий контроль.Используется 100-балльная система оценивания. Оценка работы студента в течении семестра осуществляется преподавателем в соответствии с разработанной им системой оценки учебных достижений в процессе обучения по данной дисциплине.

В рабочих программах дисциплин и практик закреплены виды текущего контроля, планируемые результаты контрольных мероприятий и критерии оценки учебный достижений.

В течение семестра преподавателем проводится не менее 3-х контрольных мероприятий, по оценке деятельности студента. Если посещения занятий по дисциплине включены в рейтинг, то данный показатель составляет не более 20% от максимального количества баллов по дисциплине.

Промежуточная аттестация. Используется 5-балльная система оценивания. Оценка работы студента по окончанию дисциплины (части дисциплины) осуществляется преподавателем в соответствии с разработанной им системой оценки достижений студента в процессе обучения по данной дисциплине. Промежуточная аттестация также проводится по окончанию формирования компетенций.

Порядок перевода рейтинга, предусмотренных системой оценивания, по дисциплине, в пятибалльную систему.

Высокий уровень – 100% - 70% - отлично, хорошо.

Средний уровень – 69% - 50% - удовлетворительно.

Показатель оценки	По 5-балльной системе	Характеристика показателя
100% - 85%	отлично	обладают теоретическими знаниями в полном объеме, понимают, самостоятельно умеют применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов на высоком уровне
84% - 70%	хорошо	обладают теоретическими знаниями в полном объеме, понимают, самостоятельно умеют применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов. Могут быть допущены недочеты, исправленные студентом самостоятельно в процессе работы (ответа и т.д.)
69% - 50%	удовлетворительно	обладают общими теоретическими знаниями, умеют применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов на среднем уровне. Допускаются ошибки, которые студент затрудняется исправить самостоятельно.
49 % и менее	неудовлетворительно	обладают не полным объемом общих теоретическими знаниями, не умеют самостоятельно применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов. Не сформированы умения и навыки для решения профессиональных задач
100% - 50%	зачтено	характеристика показателя соответствует «отлично», «хорошо», «удовлетворительно»
49 % и менее	не зачтено	характеристика показателя соответствует «неудовлетворительно»

7. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

7.1. Содержание лекций

Тема 1. Основные понятия и анализ угроз информационной безопасности. Разработка политики информационной безопасности на уровне БД ((ПК-3, ПК-4) Основные понятия защиты информации и информационной безопасности. Анализ угроз информационной безопасности и их классификация
Тема 2. Теоретические основы разработки автоматизированных средств (элементов) систем информационной безопасности. (ПК-3, ПК-4) Основы кодирования. Его цели. Оценка помеоустойчивости.Основные понятия криптографической защиты информации. Модульная арифметика, сравнения и матрицы. Алгебраические структуры (группы, кольца, поля). Простые числа и уравнения сравнения
Тема 3. Классическая криптография (ПК-3, ПК-4) Симметричные шифры замены и перестановок. Шифры: афинный, Вижинера, Хилла. Криптоанализ классических шифров.
Тема 4. Симметричные алгоритмы шифрования (ПК-3, ПК-4) Алгоритмы DES, AES, ГОСТ 28147-89
Тема 5. Хэш-функции (ПК-3, ПК-4) Одностороння функция и одностороння функция с секретом. Хэш-функции, их свойства и применение. Обзор хэш-функций SHA, Whirpool
Тема 6. Электронно-цифровая подпись (ПК-3, ПК-4) Понятия об электронно-цифровой подписи (ЭЦП). Схема формирования ЭЦП.
Тема 7. Асимметричные алгоритмы шифрования (ПК-3, ПК-4) Алгоритмы RSA, системы шифрования на эллиптических кривых
Тема 8. Стеганография и стеганоанализ (ПК-3, ПК-4) Классическая и компьютерная стенография. Методы компьютерной стеганографии. Цифровые водяные знаки. Стеганоанализ. Методы стеганоанализа
Тема 9. Уязвимости программного обеспечения (ПК-3, ПК-4) Уязвимости переполнения буфера, переполнения целочисленных значений, форматирующей строки, возвращения управления в lips. Основы работы с отладчиком и дизассемблером.
Тема 10. Компьютерные вирусы и методы их обнаружения (ПК-3, ПК-4) Классификация вредоносного программного обеспечения. Способы обнаружения компьютерных вирусов. Антивирусы
Тема 11. Разделение прав в операционных системах (ПК-3, ПК-4) Принципы построения многопользовательской операционной системы. Принципы организации безопасности на уровне операционной системы
Тема 12. Методы авторизации и аутентификации пользователей (ПК-3, ПК-4) Методы авторизации и аутентификации пользователей. Фиксированные и одноразовые пароли.
Тема 13. Безопасность сетей ЭВМ (ПК-3, ПК-4) Безопасность на прикладном, на транспортном, на сетевом уровнях. Принципы построения виртуальных защищенных сетей. Принципы работы межсетевых экранов и систем обнаружения вторжений

7.2 Содержание практических занятий и лабораторных работ

Тема 2. Теоретические основы разработки автоматизированных средств (элементов) систем информационной безопасности. (ПК-3, ПК-4) Нахождение НОД. Нахождение модульных инверсий. Нахождение обратных матриц. Испытание простоты чисел
Тема 4. Симметричные алгоритмы шифрования (ПК-3, ПК-4) Знакомство с пакетом OpenSSL
Тема 5. Хэш-функции (ПК-3, ПК-4) Симметричное шифрование. Работа с пакетом OpenSSL
Тема 14. Ассиметричные алгоритмы шифрования (продолжение) (ПК-3, ПК-4) Ассиметричное шифрование. Работа с пакетом OpenSSL
Тема 15. Стеганография и стеганоанализ (продолжение) (ПК-3, ПК-4) Текстовая стеганография. Работа с пакетом OpenPuff
Тема 16. Уязвимости программного обеспечения (продолжение) (ПК-3, ПК-4) Исследование уязвимостей программного обеспечения. Работа с программой IDA Pro
Тема 17. Компьютерные вирусы и методы их обнаружения (продолжение) (ПК-3, ПК-4) Исследование компьютерных вирусов в дизассемблере. Работа с программой IDA Pro

7.3. Содержание самостоятельной работы

Тема 2. Теоретические основы разработки автоматизированных средств (элементов) систем информационной безопасности. (ПК-3, ПК-4) Основные понятия криптографической защиты информации. Модульная арифметика, сравнения и матрицы. Алгебраические структуры (группы, кольца, поля). Простые числа и уравнения сравнения.
Тема 3. Классическая криптография (ПК-3, ПК-4) Симметричные шифры замены и перестановок. Шифры: афинный, Вижинера, Хилла. Криптоанализ классических шифров.
Тема 4. Симметричные алгоритмы шифрования (ПК-3, ПК-4) Алгоритмы DES, AES, ГОСТ 28147-89
Тема 5. Хэш-функции (ПК-3, ПК-4) Односторонняя функция и односторонняя функция с секретом. Хэш-функции, их свойства и применение. Обзор хэш-функций SHA, Whirpool

Тема 6. Электронно-цифровая подпись (ПК-3, ПК-4) Понятие об электронно-цифровая подпись (ЭЦП). Схема формирования ЭЦП.
Тема 7. Асимметричные алгоритмы шифрования (ПК-3, ПК-4) Алгоритм RSA, системы шифрования на эллиптических кривых
Тема 8. Стеганография и стеганоанализ (ПК-3, ПК-4) Классическая и компьютерная стеганография. Методы компьютерной стеганографии. Цифровые водяные знаки. Стеганоанализ. Методы стеганоанализа
Тема 9. Уязвимости программного обеспечения (ПК-3, ПК-4) Уязвимости переполнения буфера, переполнения целочисленных значений, форматирующей строки, возвращения управления в libc. Основы работы с отладчиком и дизассемблером
Тема 17. Компьютерные вирусы и методы их обнаружения (продолжение) (ПК-3, ПК-4) Классификация вредоносного программного обеспечения. Способы обнаружения компьютерных вирусов. Антивирусы
Тема 18. Разделение прав в операционных системах (продолжение) (ПК-3, ПК-4) Принципы построения многопользовательской операционной системы. Принципы организации безопасности на уровне операционной системы
Тема 19. Методы авторизации и аутентификации пользователей (продолжение) (ПК-3, ПК-4) Методы авторизации и аутентификации пользователей. Фиксированные и одноразовые пароли
Тема 20. Безопасность сетей ЭВМ (продолжение) (ПК-3, ПК-4) Безопасность на прикладном, на транспортном, на сетевом уровнях. Принципы построения виртуальных защищенных сетей. Принципы работы межсетевых экранов и систем обнаружения вторжений

7.3.1. Примерные вопросы для самостоятельной подготовки к зачету/экзамену
Приложение 1

7.3.2. Практические задания по дисциплине для самостоятельной подготовки к зачету/экзамену
Приложение 2

7.3.3. Перечень курсовых работ
Материалы не предусмотрены

7.4. Электронное портфолио обучающегося
Материалы не размещаются

7.5. Методические рекомендации по выполнению контрольной работы
Материалы не предусмотрены

7.6 Методические рекомендации по выполнению курсовой работы
Материалы не предусмотрены

8. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

По заявлению студента

В целях доступности освоения программы для лиц с ограниченными возможностями здоровья при необходимости кафедра обеспечивает следующие условия:

- особый порядок освоения дисциплины, с учетом состояния их здоровья;
- электронные образовательные ресурсы по дисциплине в формах, адаптированных к ограничениям их здоровья;
- изучение дисциплины по индивидуальному учебному плану (вне зависимости от формы обучения);
- электронное обучение и дистанционные образовательные технологии, которые предусматривают возможности приема-передачи информации в доступных для них формах.
- доступ (удаленный доступ), к современным профессиональным базам данных и информационным справочным системам, состав которых определен РПД.

9. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Сайт библиотеки УрГЭУ
http://lib.usue.ru/

Основная литература:

2. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах [Электронный ресурс]:Учебное пособие. - Москва: Издательский Дом "ФОРУМ", 2022. - 592 – Режим доступа: https://znanium.com/catalog/product/1843022

3. Ищейнов В. Я., Мецатунян М. В. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации [Электронный ресурс]:учебное пособие. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2022. - 256 – Режим доступа: https://znanium.ru/catalog/product/1861659

4. Гришина Н. В. Основы моделирования процессов и систем защиты информации [Электронный ресурс]:Учебное пособие. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2022. - 107 – Режим доступа: https://znanium.com/catalog/product/1891122

Дополнительная литература:

10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ЛИЦЕНЗИОННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ, ОНЛАЙН КУРСОВ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Перечень лицензионного программного обеспечения:

Microsoft Windows 10 .Договор № 52/223-ПО/2020 от 13.04.2020, Акт № Tr000523459 от 14.10.2020. Срок действия лицензии -Без ограничения срока.

Microsoft Office 2016.Договор № 52/223-ПО/2020 от 13.04.2020, Акт № Tr000523459 от 14.10.2020 Срок действия лицензии -Без ограничения срока.

Adobe Reader. Лицензия freeeware. Срок действия лицензии - без ограничения срока.

Secret Net 7. Клиент (автономный режим работы). Договор № 73700092 от 04.08.2017, Товарная накладная № 73700092 от 11.10.2017.

hMailServer. Лицензия AGPL. Срок действия лицензии - без ограничения срока.

Microsoft Visual Studio Community. Лицензия для образовательных учреждений. Срок действия лицензии - без ограничения срока.

Перечень информационных справочных систем, ресурсов информационно-телекоммуникационной сети «Интернет»:

11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Реализация учебной дисциплины осуществляется с использованием материально-технической базы УрГЭУ, обеспечивающей проведение всех видов учебных занятий и научно-исследовательской и самостоятельной работы обучающихся:

Специальные помещения представляют собой учебные аудитории для проведения всех видов занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду УрГЭУ.

Все помещения укомплектованы специализированной мебелью и оснащены мультимедийным оборудованием спецоборудованием (информационно-телекоммуникационным, иным компьютерным), доступом к информационно-поисковым, справочно-правовым системам, электронным библиотечным системам, базам данных действующего законодательства, иным информационным ресурсам служащими для представления учебной информации большой аудитории.

Для проведения занятий лекционного типа презентации и другие учебно-наглядные пособия, обеспечивающие тематические иллюстрации.

Приложение 1
к рабочей программе

Федеральное государственное бюджетное образовательное учреждение высшего образования
УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ

УТВЕРЖДЕНЫ
на заседании шахматного искусства и
компьютерной математики

Перечень вопросов для подготовки к зачету и экзамену по дисциплине

Информационная безопасность телекоммуникационных систем

направление подготовки **02.03.03 Математическое обеспечение и администрирование информационных систем**
профиль **Прикладной искусственный интеллект**

Вопросы к зачету

1. Научные и законодательные определения информации. Соотношение понятий «информация», «документированная информация», «информационные ресурсы», «документ».
2. Сущность и понятие информационной безопасности. Связь информационной безопасности с информатизацией общества.
3. Основные положения доктрины информационной безопасности Российской Федерации и их реализация.
4. Сущность и понятие защиты информации.
5. Уязвимость информации. Цели защиты информации.
6. Понятие и виды конфиденциальной информации в современном российском законодательстве.
7. Государственная тайна, ее нормативное регулирование.
8. Правовой режим персональных данных. Общая характеристика Федерального закона «О персональных данных».
9. Понятие коммерческой тайны. Общая характеристика Федерального закона «О коммерческой тайне».
10. Понятие и разновидности служебной и профессиональной тайн.
11. Перечень конфиденциальных сведений и Перечень конфиденциальных документов, методика их формирования.
12. Система информационной безопасности как подсистема корпоративной. Цели, состав, ресурсы
13. Классификация ресурсов системы ИБ.
14. Понятие информации, её свойства. Соотношение понятий «информация», «документированная информация», «информационные ресурсы», «документ».
15. Защита информации. Информационная система и система ИБ как подсистемы корпоративной. Их соотношение.
16. Организационные компоненты системы ИБ. внешнее и внутреннее законодательство
17. Политика безопасности как компонент системы ИБ. Элементы и структура, классификация элементов политики безопасности,
18. Структура политики безопасности организации: базовая политика,
19. Специализированные политики, процедуры безопасности
20. Разработка политики безопасности организации.
21. Количественная и качественная оценки безопасности
22. Классификация угроз информационной безопасности
23. Угрозы и уязвимости беспроводных сетей
24. Способы обеспечения защиты информации в беспроводных сетях
25. Методы аутентификации, использующие пароли. Виды паролей
26. Методы строгой аутентификации. Их виды
27. Виды биометрической аутентификации
28. Управление идентификацией и доступом. SSO (Single Sign- On)
29. Основные типы угроз СУБД.
30. Методы и средства зашиты СУБД.
31. Обеспечение конфиденциальности и целостности электронных документов.

Вопросы к экзамену

1. Служба конфиденциального делопроизводства, ее статус в структуре организации.
2. Квалификационные характеристики и требования к сотрудникам службы конфиденциального делопроизводства.
3. Цели и задачи, права и обязанности, нормативно-методическая база службы конфиденциального делопроизводства.
4. Анализ угроз несанкционированного получения документированной информации, хищения или уничтожения документов, их фальсификации или подмены.
5. Предполагаемые рубежи и уровни защиты документопотоков
6. Понятие «защищенный документооборот», его цели и задачи.
7. Гриф ограничения доступа к документу: понятие, назначение, виды.
8. Избирательность и разрешительная система доступа к конфиденциальным документам.
9. Прием и регистрация конфиденциальных документов.
10. Принципы и этапы документирования конфиденциальных сведений.
11. Учетные формы: виды, правила оформления и ведения.
12. Составление, учет и уничтожение проектов конфиденциальных документов.
13. Особенности оформления реквизитов конфиденциальных документов.
14. Правила издания, копирования и тиражирования конфиденциальных документов
15. Экспедиционная обработка исходящих конфиденциальных документов.
16. Организация и контроль исполнения конфиденциальных документов. Правила работы исполнителя.
17. Экспертиза ценности конфиденциальных документов
18. Номенклатура конфиденциальных дел. Установление сроков конфиденциальности при составлении номенклатуры дел.
19. Правила формирования и оформления конфиденциальных дел.
20. Учет выдачи дел во временное пользование.
21. Подготовка конфиденциальных дел и документов для архивного хранения.
22. Цели кодирования. Требования, предъявляемые при кодирования.
23. Понятие кодирования. Кодовый алфавит, значность кода. Виды: равномерные и неравномерные, простые и корректирующие.
24. Шифрование как вид кодирования, Его цели. Помехостойкость и криптостойкость, способы их оценки.
25. Симметричные криптосистемы шифрования. Особенности их применения, достоинства и недостатки
26. Асимметричные криптосистемы шифрования. Особенности их применения, достоинства и недостатки.
27. ЭЦП. Основные процедуры цифровой подписи.
28. Функции хэширования. Требования, предъявляемые к хэш-функциям. Области применения

Приложение 2
к рабочей программе

7.3.2. Практические задания по дисциплине для самостоятельной подготовки к зачету/экзамену

5 **семестр**

№	Содержание задания	Проверяемая компетенция
1	Даны символы a, b, c, d с частотами f_a = 0,5; f_b = 0,25; f_c = 0,125; f_d= 0,125. Построить эффективный код методом Шеннона-Фано.	ПК-3, ПК-4
2	Реализовать шифрование фразы «БЕЗОПАСНОСТЬ – ЭТО ПРОФЕССИЯ» шифром Виженера. Ключ – «СЕЙФ».	ПК-3, ПК-4
3	Используя шифр Полибия, дешифровать криптограмму: T = ЕС ИМ АНУШ АЙАСТАНИ АРЕВААМ БАРН ЭМ СИРУМ МЕР ЙИН САЗИ ВОГБАНВАГ ЛАЦАКУМАЦ ЛАРН ЭМ СИРУМ	ПК-3, ПК-4
4	Даны символы a и b с частотами 0,9 и 0,1, соответственно. Построить эффективный код методом Шеннона-Фано для блоков из двух символов (n = 2).	ПК-3, ПК-4
5	Расшифровать сообщение T=FBRTLWUGAJQINZTHHXTEPHBNXSW, зашифрованное линейным шифрующим преобразованием триграмм 26-буквенного алфавита A-Z с числовыми эквивалентами 0-25. Известно, что последние три триграммы - это подпись отправителя JAMESBOND. Найти дешифрующую матрицу и прочитать сообщение.	ПК-3, ПК-4

6 семестр

№	Содержание задания	Проверяемая Компетенция
1	Вычислить вручную значение a^b(mod c) для a = 9928, b = 413, c = 82224.	ПК-3, ПК-4

2	Для точек P, Q, R эллиптической кривой $E_{751}(-1,1)$ найти точку 2P + 3Q – R, если P = (58, 139), Q = (67, 667), R = (82, 481).	ПК-3, ПК-4
3	Вычислить хеш массива y = {5 9 12 34 32 45 67 79 101}. Алгоритм – MD5.	ПК-3, ПК-4
4	Найти обратное значение числа по модулю $x = 9^{-1} \pmod 5$. при помощи определения кратности k («по определению»).	ПК-3, ПК-4
5	Реализовать простую ЭЦП без контроля целостности с использованием алгоритма RSA.	ПК-3, ПК-4
6	Реализовать шифрование фразы «МЫ ИЗУЧАЕМ ШИФР» шифром Кардано.	ПК-3, ПК-4