МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования

"САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ"

Кафедра № 14

УТВЕРЖДАЮ
Руководитель образовательной программы

к.т.н.,доц.
(должность, уч. степень, звание)

В.Л. Оленев
(инициалы, фамилия)

(подпись)

«05» февраля 2026 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Предпрофессиональная подготовка»
(Наименование дисциплины)

Код направления подготовки/ специальности	09.03.01
Наименование направления подготовки/ специальности	Информатика и вычислительная техника
Наименование направленности/ специализации	Программные системы анализа, обработки и передачи данных
Форма обучения	очная
Год приема	2026

Санкт-Петербург– 2026

Лист согласования рабочей программы дисциплины

Программу составил (а)

доц.,к.т.н. (должность, уч. степень, звание) — (подпись, дата) — А.В. Шахомиров (инициалы, фамилия)

Программа одобрена на заседании кафедры № 14
«05» февраля 2026 г, протокол № 5

Заведующий кафедрой № 14

к.т.н.,доц. (уч. степень, звание) — (подпись, дата) — В.Л. Оленев (инициалы, фамилия)

Заместитель директора института №1 по методической работе

доц.,к.т.н. (должность, уч. степень, звание) — (подпись, дата) — В.Е. Таратун (инициалы, фамилия)

Аннотация

Дисциплина «Предпрофессиональная подготовка» входит в образовательную программу высшего образования – программу бакалавриата по направлению подготовки/ специальности 09.03.01 «Информатика и вычислительная техника» направленности/специализации «Программные системы анализа, обработки и передачи данных». Дисциплина реализуется кафедрой «№14».

Дисциплина не является обязательной при освоении обучающимся образовательной программы и направлена на углубленное формирование следующих компетенций:

ОПК-2 «Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности»

ПК-0 «Способен выстраивать и реализовывать траекторию профессионального саморазвития»

Содержание дисциплины охватывает круг вопросов, связанных с оформлением и компоновкой технической документации, подготовкой и использованием интерфейсной графики, использованием программного обеспечения в профессиональной деятельности, а также с разработкой алгоритмов и компьютерных программ, пригодных для практического применения.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: *практические занятия, самостоятельная работа обучающегося*.

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости, промежуточная аттестация в форме зачета (3 семестр), дифференцированного зачета (4 семестр).

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 часа.

Язык обучения по дисциплине «русский »

1. Перечень планируемых результатов обучения по дисциплине

1.1. Цели преподавания дисциплины - формирование базовой системы знаний, умений и навыков в области обработки информации, как фундаментального раздела естественной науки, имеющей собственный объект – информацию, свою предметную область -информационные процессы и информационные системы и развивающую метод исследования, присущий только ей – информационный подход, как фундаментальный метод научного познания.

1.2. Дисциплина является факультативной дисциплиной по направлению образовательной программы высшего образования (далее – ОП ВО).

1.3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОП ВО.

В результате изучения дисциплины обучающийся должен обладать следующими компетенциями или их частями. Компетенции и индикаторы их достижения приведены в таблице 1.

Таблица 1 – Перечень компетенций и индикаторов их достижения

Категория (группа) компетенции	Код и наименование компетенции	Код и наименование индикатора достижения компетенции
Общепрофессиональные компетенции	ОПК-2 Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности	ОПК-2.У.1 уметь выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности ОПК-2.В.1 владеть навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности
Профессиональные компетенции	ПК-0 Способен выстраивать и реализовывать траекторию профессионального саморазвития	ПК-0.З.1 знать направления профессионального развития, в том числе инновационные ПК-0.У.1 уметь ставить себе образовательные цели под возникающие профессиональные задачи ПК-0.В.1 владеть инструментами различных направлений профессионального развития, в том числе цифровыми

2. Место дисциплины в структуре ОП

Дисциплина может базироваться на знаниях, ранее приобретенных обучающимися при изучении следующих дисциплин:

- «Основы цифровой грамотности»
- «Основы проектной деятельности в профессии»

3. Объем и трудоемкость дисциплины

Данные об общем объеме дисциплины, трудоемкости отдельных видов учебной работы по дисциплине (и распределение этой трудоемкости по семестрам) представлены в таблице 2.

Таблица 2 – Объем и трудоемкость дисциплины

Вид учебной работы	Всего	Трудоемкость по семестрам	
		№3	№4
1	2	3	4
Общая трудоемкость дисциплины, ЗЕ/ (час)	4/ 144	2/ 72	2/ 72
Из них часов практической подготовки			
Аудиторные занятия, всего час.	68	34	34
в том числе:			
лекции (Л), (час)			
практические/семинарские занятия (ПЗ), (час)	68	34	34
лабораторные работы (ЛР), (час)			
курсовой проект (работа) (КП, КР), (час)			
экзамен, (час)			
Самостоятельная работа, всего (час)	76	38	38
Вид промежуточной аттестации: зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.)	Зачет, Дифф. зач.,	Зачет,	Дифф. зач.,

4. Содержание дисциплины

4.1. Распределение трудоемкости дисциплины по разделам и видам занятий.

Разделы, темы дисциплины и их трудоемкость приведены в таблице 3.

Таблица 3 – Разделы, темы дисциплины, их трудоемкость

Разделы, темы дисциплины	Лекции (час)	ПЗ (СЗ) (час)	ЛР (час)	КП/КР (час)	СР (час)
Семестр 3					
Раздел 1. Измерение количества информации		6			12
Раздел 2. Пропускная способность каналов		4			12
Раздел 3. Краткие сведения из алгебры прикладной информатики		24			14
Итого в семестре:		34			38
Семестр 4					
Раздел 4. Теория оптимального кодирования		16			19
Раздел 5. Криптографические методы защиты информации		18			19
Итого в семестре:		34			38
Итого	0	68	0	0	76

Практическая подготовка заключается в непосредственном выполнении обучающимися определенных трудовых функций, связанных с будущей профессиональной деятельностью.

4.2. Содержание разделов и тем лекционных занятий.

Содержание разделов и тем лекционных занятий приведено в таблице 4.

Таблица 4 – Содержание разделов и тем лекционного цикла

Номер раздела	Название и содержание разделов и тем лекционных занятий
	Учебным планом не предусмотрено

4.3. Практические (семинарские) занятия

Темы практических занятий и их трудоемкость приведены в таблице 5.

Таблица 5 – Практические занятия и их трудоемкость

№ п/п	Темы практических занятий	Формы практических занятий	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Семестр 3					
1	Элементы теории информации. Краткие сведения по теории вероятностей. Формула Байеса. Сравнение способов принятия решений.	Практическое занятие	2	2	1
2	Информационные процессы. Типовые модели обработки информации. Количество информации и его свойства.	Практическое занятие	2	2	1
3	Методы алгоритмизации информационных процессов. Источники информации. Количество собственной информации источников.	Практическое занятие	2	2	1
4	Энтропия. Свойства энтропии. Физическая интерпретация. Множественные источники информации.	Практическое занятие	2	2	2
5	Основы моделирования и модели информатики. Средняя взаимная информация. Пропускная способность каналов. Примеры вычисления пропускной способности. Полнота использования пропускной способности в прикладной информатике.	Практическое занятие	2	2	2
6	Алгебраический язык прикладной информатики. Понятия группы, поля, кольца. Алгоритм Эвклида.	Практическое занятие	4	4	3
7	Свойства конечных полей. Линейная независимость, базис и правила вычислений в конечных полях.	Практическое занятие	5	5	3
8	Кольцо полиномов над конечными полями, идеалы. Примеры вычислений. Использование пакетов прикладных программ.	Практическое занятие	5	5	3

9	Методы кодирования информации. Помехоустойчивые коды. Линейные коды. Границы Хемминга и Варшамова. Основные свойства проверочных и порождающих матриц.	Практическое занятие	5	5	3
10	Логические основы информатики (автоматная теория компьютера). Понятие об алгоритмах кодирования и декодирования информации. Управление в компьютере на примерах простейших алгоритмов кодирования и декодирования.	Практическое занятие	5	5	3
Семестр 4					
11	Практическое освоение классификационных моделей: иерархических, тезаурусных, алфавитно-предметных и т.п.. Древовидные модели. Кодирование сообщений кодами переменной длины. Алгоритм Хаффмана и его обобщения.	Практическое занятие	8	8	4
12	Дальнейшее развитие прикладной теории алгоритмов. Анализ алгоритмов кодирования сообщений кодами постоянной длины. Сравнение способов кодирования.	Практическое занятие	8	8	4
13	Актуальность криптографической защиты информации. Примеры криптографической защиты. Модульная арифметика. Китайская теорема об остатках. Применение китайской теоремы об остатках в задачах криптографии. Системы RSA.	Практическое занятие	9	9	5
14	Представление о потоковых шифрах. Алгоритмы генерации потоковых шифров. Области применения криптографических методов. Защита информации в сети GSM.	Практическое занятие	9	9	5
Всего			68		

4.4. Лабораторные занятия

Темы лабораторных занятий и их трудоемкость приведены в таблице 6.

Таблица 6 – Лабораторные занятия и их трудоемкость

№ п/п	Наименование лабораторных работ	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Учебным планом не предусмотрено				
Всего				

4.5. Выполнение курсового проекта/ курсовой работы

Учебным планом не предусмотрено

4.6. Самостоятельная работа обучающихся

Виды самостоятельной работы и ее трудоемкость приведены в таблице 7.

Таблица 7 – Виды самостоятельной работы и ее трудоемкость

Вид самостоятельной работы	Всего, час	Семестр 3, час	Семестр 4, час
1	2	3	4
Изучение теоретического материала дисциплины (ТО)		10	10
Курсовое проектирование (КП, КР)			
Расчетно-графические задания (РГЗ)			
Выполнение реферата (Р)			
Подготовка к текущему контролю успеваемости (ТКУ)		8	8
Домашнее задание (ДЗ)			
Контрольные работы заочников (КРЗ)			
Подготовка к промежуточной аттестации (ПА)		20	20
Всего:	76	38	38

5. Перечень учебно-методического обеспечения

6. для самостоятельной работы обучающихся по дисциплине (модулю)

Учебно-методические материалы для самостоятельной работы обучающихся указаны в п.п. разделов 6-11.

7. Перечень печатных и электронных учебных изданий

Перечень печатных и электронных учебных изданий приведен в таблице 8.

Таблица 8– Перечень печатных и электронных учебных изданий

Шифр/ URL адрес	Библиографическая ссылка	Количество экземпляров в библиотеке (кроме электронных экземпляров)
621.391(075)	Кудряшов Б.Д. Теория информации: учебное пособие/ Б. Д. Кудряшов. - СПб.: ПИТЕР, 2009. - 320 с	80
519.7.К89	Кузнецов О.П. Дискретная математика для инженера. - 4-е изд., стер.. - СПб.: Лань, 2005. - 395 с.:	10

	Алутина Е.Ф., Румянцев И.А. «Теоретическая информатика». Учебное пособие под общей редакцией д.т.н. профессора Румянцева И.А., Благовещенск: Изд. БГПУ, 2005,361 с	
	Румянцев И.А. «Прикладная теория алгоритмов». Учебное пособие для студентов педагогических вузов. Спб. Изд. «Образование», 2004, 207 с.	
	Возенкрафт Д., Джекобс И. «Теоретические основы техники связи». М.: изд. «Мир», 1969, 407 с	
	Грэхем Р., Кнут Д., Поташник О. Конкретная математика. М.:Мир, 1998.	
	Акритас А. Основы компьютерной алгебры с приложениями. М., Мир, 1994	
	Крук Е.А., Овчинников А.А. Методы программирования и прикладные алгоритмы. Учебное пособие. - Санкт-Петербург, ГУАП, 2007, 165 с.	

8. Перечень электронных образовательных ресурсов

9. информационно-телекоммуникационной сети «Интернет»

Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины приведен в таблице 9.

Таблица 9 – Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет»

URL адрес	Наименование
lms.guap.ru/	LMS ГУАП

10. Перечень информационных технологий

10.1. Перечень программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине.

Перечень используемого программного обеспечения представлен в таблице 10.

Таблица 10– Перечень программного обеспечения

№ п/п	Наименование
	Не предусмотрено

10.2. Перечень информационно-справочных систем, используемых при осуществлении образовательного процесса по дисциплине

Перечень используемых информационно-справочных систем представлен в таблице 11.

Таблица 11– Перечень информационно-справочных систем

№ п/п	Наименование
	Не предусмотрено

11. Материально-техническая база

Состав материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине, представлен в таблице12.

Таблица 12 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы	Номер аудитории (при необходимости)
1	Компьютерный класс	
2	Читальный зал	
3	Библиотека	

12. Оценочные средства для проведения промежуточной аттестации

12.1. Состав оценочных средствдля проведения промежуточной аттестации обучающихся по дисциплине приведен в таблице 13.

Таблица 13 – Состав оценочных средств для проведения промежуточной аттестации

Вид промежуточной аттестации	Перечень оценочных средств
Дифференцированный зачёт	Список вопросов; Тесты.
Зачет	Список вопросов; Тесты.

12.2. В качестве критериев оценки уровня сформированности (освоения) компетенций обучающимися применяется 5-балльная шкала оценки сформированности компетенций, которая приведена в таблице 14. В течение семестра может использоваться 100-балльная шкала модульно-рейтинговой системы Университета, правила использования которой, установлены соответствующим локальным нормативным актом ГУАП.

Таблица 14 –Критерии оценки уровня сформированности компетенций

Оценка компетенции 5-балльная шкала	Характеристика сформированных компетенций
«отлично» «зачтено»	Обучающийся: – глубоко и всесторонне усвоил программный материал; – уверенно, логично, последовательно и грамотно его излагает; – опираясь на знания основной и дополнительной литературы, тесно связывает усвоенные научные положения с практической деятельностью направления; – умело обосновывает и аргументирует выдвигаемые им идеи; – делает выводы и обобщения; – свободно владеет системой специализированных понятий. – правильно выполнил от 90% до 100% тестовых заданий**.
«хорошо» «зачтено»	Обучающийся: – твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы; – не допускает существенных неточностей; – увязывает усвоенные знания с практической деятельностью направления; – аргументирует научные положения; – делает выводы и обобщения; – владеет системой специализированных понятий. – правильно выполнил от 70% до 89% тестовых заданий**.

Оценка компетенции 5-балльная шкала	Характеристика сформированных компетенций
«удовлетворительно» «зачтено»	– обучающийся усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; – допускает несущественные ошибки и неточности; – испытывает затруднения в практическом применении знаний направления; – слабо аргументирует научные положения; – затрудняется в формулировании выводов и обобщений; – частично владеет системой специализированных понятий. – правильно выполнил от 51% до 69% тестовых заданий**.
«неудовлетворительно» «не зачтено»	– обучающийся не усвоил значительной части программного материала; – допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении; – испытывает трудности в практическом применении знаний; – не может аргументировать научные положения; – не формулирует выводов и обобщений. – правильно выполнил менее 51% тестовых заданий**.

12.3. Типовые контрольные задания или иные материалы.

Вопросы (задачи) для экзамена представлены в таблице 15.

Таблица 15 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена	Код индикатора
	Учебным планом не предусмотрено	

Вопросы (задачи) для зачета / дифф. зачета представлены в таблице 16.

Таблица 16 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифф. зачета	Код индикатора
семестр 3		
1	Формула Байеса и принятие решений. Сформулируйте задачу проверки гипотез при наличии двух альтернатив. Выведите формулу Байеса для апостериорной вероятности. В чем состоит байесовский подход к сравнению способов принятия решений (приведите пример минимизации средней стоимости ошибки)?	ПК-0.3.1, ПК-0.У.1, ПК-0.В.1
2	Модели обработки информации. Дайте определение типовой модели обработки информации (например, модель «черного ящика», детерминированная или стохастическая модель). В чем разница между обработкой сигнала и обработкой данных с точки зрения семантики информации?	ПК-0.3.1, ПК-0.У.1, ПК-0.В.1
3	Количество информации и его свойства. Дайте определение количества информации по Хартли и по Шеннону. Перечислите основные аксиоматические свойства меры количества информации (аддитивность, непрерывность, монотонность). Приведите пример, где эти меры дают разный результат.	ПК-0.3.1, ПК-0.У.1, ПК-0.В.1
4	Источники информации и собственная информация. Определите понятие «собственная информация» отдельного сообщения (surprisal). Как она зависит от вероятности события? Выведите формулу для количества собственной информации источника с памятью (марковский источник) по сравнению с источником без памяти.	ПК-0.3.1, ПК-0.У.1, ПК-0.В.1
5	Свойства энтропии. Сформулируйте и докажите основное свойство энтропии: $H(X) \leq \log_2 n$ (максимум достигается при равномерном	ПК-0.3.1, ПК-0.У.1, ПК-0.В.1
	распределении). В чем состоит физическая интерпретация энтропии как меры неопределенности (или хаоса) в прикладной информатике?	
6	Множественные источники. Дайте определение условной энтропии $H(X \mid Y)$ и совместной энтропии $H(X,Y)$. Запишите цепное правило для энтропии. Как с помощью этих понятий оценить избыточность языка (естественного или машинного)?	ПК-0.3.1, ПК-0.У.1, ПК-0.В.1
7	Физическая интерпретация энтропии. Сравните термодинамическую энтропию (больцмановскую) и информационную энтропию Шеннона. Приведите пример, демонстрирующий, что потеря информации (стирание данных) ведет к возрастанию физической энтропии (парадокс Максвелла).	ПК-0.3.1, ПК-0.У.1, ПК-0.В.1
8	Средняя взаимная информация. Дайте строгое определение средней взаимной информации $I(X;Y)$. Докажите, что $I(X;Y) \geq 0$ (неотрицательность). При каком условии канал считается "бесшумным" с точки зрения взаимной информации?	ПК-0.3.1, ПК-0.У.1, ПК-0.В.1
9	Пропускная способность канала. Дайте определение пропускной способности C канала. Выведите формулу для пропускной способности двоичного симметричного канала (ДСК) с вероятностью ошибки p. Почему в прикладной информатике важно стремиться к полноте использования пропускной способности (принцип Шеннона)?	ОПК-2.У.1
10	Примеры вычисления. Рассчитайте пропускную способность канала с расширением (Z-канала) или канала с удалением (стиранием). Опишите алгоритм вычисления для каналов с памятью (на примере).	ОПК-2.В.1
11	Алгебраический язык. Дайте определения группы, кольца и поля. Приведите примеры конечных и бесконечных полей. В чем состоит алгоритм Евклида и как он применяется для нахождения обратного элемента в кольце вычетов по модулю простого числа?	ПК-0.3.1, ПК-0.У.1, ПК-0.В.1
12	Конечные поля $GF(2^m)$. Сформулируйте свойства конечных полей (характеристика, порядок). Дайте определение линейной независимости элементов поля относительно основного поля $GF(2)$. Как построить базис расширенного поля $GF(2^m)$?	ПК-0.3.1, ПК-0.У.1, ПК-0.В.1
13	Правила вычислений в конечных полях. Покажите, как выполняется сложение и умножение в поле $GF(2^3)$ (по модулю примитивного полинома). В чем отличие вычислений в поле характеристики 2 от обычной арифметики?	ОПК-2.В.1
14	Кольцо полиномов и идеалы. Дайте определение кольца полиномов $F[x]$ над конечным полем. Что такое идеал кольца? Как связаны идеалы и порождающие полиномы в теории циклических кодов? Приведите пример вычисления в кольце полиномов с использованием пакетов прикладных программ (например, Matlab или символьной математики).	ПК-0.3.1, ПК-0.У.1, ПК-0.В.1
15	Помехоустойчивые и линейные коды. Дайте определение линейного кода $[n, k, d]$. В чем разница между систематическими и несистематическими кодами? Сформулируйте основные свойства проверочной матрицы H и порождающей матрицы G (включая условие ортогональности $G \cdot H^T = 0$).	ОПК-2.У.1
16	Границы Хемминга и Варшамова. Сформулируйте границу Хемминга (сферической упаковки) для корректирующей способности t. Сформулируйте границу Варшамова-Гилберта (существования). В чем принципиальное различие этих двух границ: одна дает верхнюю оценку (ограничение), вторая — нижнюю (гарантия существования)?	ПК-0.3.1, ПК-0.У.1, ПК-0.В.1
17	Порождающие и проверочные матрицы. Как по проверочной матрице определить синдром ошибки? Объясните алгоритм декодирования по	ОПК-2.В.1

	синдрому для линейного кода. Приведите пример вычисления синдрома для простого (7,4) кода Хемминга.	
18	Автоматная теория и алгоритмы. Дайте понятие конечного автомата как модели управления в компьютере. Опишите алгоритм кодирования на основе сверточных кодов (или кодера Рида-Соломона) как последовательного автомата. Чем отличается алгоритм кодирования от алгоритма декодирования?	ОПК-2.У.1
19	Управление на примерах. Приведите конкретный пример простейшего алгоритма декодирования (например, декодирование с помощью мажоритарной логики или алгоритм Витерби). Как в этом алгоритме реализуется управление потоком данных и синхронизация в компьютере?	ОПК-2.В.1
20	Сравнительная задача. Сравните сложность реализации алгоритмов кодирования и декодирования на примере линейного (блочного) кода и сверточного кода. Объясните, почему для коррекции пакетов ошибок чаще используют коды Рида-Соломона (алгебраическое декодирование), а для независимых ошибок — сверточные коды (вероятностное декодирование), и как это связано со свойствами конечных полей.	ПК-0.З.1, ПК-0.У.1, ПК-0.В.1
семестр 4		
1	Опишите иерархическую классификационную модель. Приведите пример её использования в электронных каталогах или базах знаний. В чём её отличие от тезаурусной модели (где связи между понятиями задаются семантически)?	ПК-0.З.1, ПК-0.У.1, ПК-0.В.1
2	Дайте определение алфавитно-предметной классификации. Приведите пример классификации документов по алфавитно-предметному принципу. Сравните её с иерархической моделью с точки зрения удобства поиска.	ПК-0.З.1, ПК-0.У.1, ПК-0.В.1
3	Что такое древовидная модель данных? Как она связана с иерархическими классификациями? Постройте дерево классификации для некоторой предметной области (например, животные, автомобили или программное обеспечение).	ПК-0.З.1, ПК-0.У.1, ПК-0.В.1
4	Объясните принцип кодирования сообщений кодами переменной длины. В чём их преимущество перед кодами постоянной длины? Приведите пример, когда использование переменной длины даёт выигрыш в средней длине кода.	ПК-0.З.1, ПК-0.У.1, ПК-0.В.1
5	Опишите алгоритм Хаффмана для построения оптимального префиксного кода. Примените его к множеству символов с вероятностями: $0.4,0.3,0.15,0.1,0.05$. Покажите построение дерева и полученные коды.	ОПК-2.В.1
6	Какие обобщения алгоритма Хаффмана существуют? Расскажите об адаптивном (динамическом) алгоритме Хаффмана и о блочном кодировании (кодирование групп символов). В каких ситуациях они предпочтительнее классического алгоритма?	ПК-0.З.1, ПК-0.У.1, ПК-0.В.1
7	Проведите сравнительный анализ кодирования постоянной длины и переменной длины. Оцените эффективность каждого подхода при разных распределениях вероятностей (равномерном и сильно неравномерном). Когда выгодно использовать постоянную длину?	ОПК-2.У.1
8	В чём состоит актуальность криптографической защиты информации в современном мире? Приведите не менее трёх примеров реальных угроз, которые нейтрализуются криптографическими методами (например, перехват, подделка, утечка данных).	ПК-0.З.1, ПК-0.У.1, ПК-0.В.1
9	Опишите основные операции модульной арифметики: сравнение по модулю, сложение, умножение, возведение в степень. Вычислите $17^{23} mod 13$ и $5^{-1} mod 7$ (обратный элемент).	ОПК-2.В.1
10	Сформулируйте Китайскую теорему об остатках (КТО). Приведите пример решения системы: $\begin{cases} x \equiv 2(\mathrm{mod}3) \\ x \equiv 3(\mathrm{mod}5) \\ x \equiv 2(\mathrm{mod}7) \end{cases}$ (найдите наименьшее неотрицательное решение).	ОПК-2.В.1
11	Объясните, как Китайская теорема об остатках применяется в криптосистеме RSA для ускорения операций расшифрования и подписи (метод Гаусса или использование CRT-версии RSA). В чём выигрыш в скорости?	ОПК-2.У.1
12	Опишите полный алгоритм криптосистемы RSA: генерация ключей, шифрование и расшифрование. Докажите корректность расшифрования на основе теоремы Эйлера. Обоснуйте стойкость RSA задачей факторизации больших чисел.	ПК-0.З.1, ПК-0.У.1, ПК-0.В.1
13	Приведите конкретный числовой пример RSA (выберите простые числа $p = 3, q = 11$), вычислите n, $\varphi(n)$, выберите открытую экспоненту e, найдите закрытую d, зашифруйте и расшифруйте сообщение $m = 7$.	ОПК-2.В.1
14	Что такое потоковые шифры? В чём их принципиальное отличие от блочных шифров? Назовите достоинства и недостатки потоковых шифров. Приведите известные примеры (RC4, A5/1).	ПК-0.З.1, ПК-0.У.1, ПК-0.В.1
15	Опишите алгоритм генерации потокового шифра на основе регистра сдвига с линейной обратной связью (РСЛОС/LFSR). Как выбирается обратная связь? В чём уязвимость линейных РСЛОС и как её преодолевают (нелинейные комбинации)?	ПК-0.З.1, ПК-0.У.1, ПК-0.В.1
16	Какие ещё методы генерации потоковых шифров существуют? Расскажите о генераторах на основе регистров с нелинейной обратной связью (NLFSR), о схеме «объединение нескольких РСЛОС» (например, генератор Геффе) и о поточных шифрах на основе блочных (режимы CTR, OFB).	ПК-0.З.1, ПК-0.У.1, ПК-0.В.1
17	Перечислите основные области применения криптографических методов в информационной безопасности. Приведите примеры использования в банковской сфере (защита платежей), государственных коммуникациях, защите корпоративных сетей, облачных хранилищах.	ПК-0.З.1, ПК-0.У.1, ПК-0.В.1
18	Опишите систему криптографической защиты информации в сетях стандарта GSM. Какие алгоритмы применяются (A5/1, A5/3) и для чего они служат? Расскажите о процедурах аутентификации абонента и шифрования трафика.	ПК-0.З.1, ПК-0.У.1, ПК-0.В.1
19	Сравните системы RSA и потоковые шифры по следующим критериям: производительность (скорость шифрования/расшифрования), область применения (обмен ключами vs. потоковые данные), криптостойкость и уязвимости.	ОПК-2.У.1
20	Предложите решение задачи: задан текст (например, «информатика и кодирование»). Постройте код Хаффмана для частот букв в этом тексте, вычислите среднюю длину кода и коэффициент сжатия по сравнению с равномерным 8-битным кодированием. Или, по выбору, решите систему сравнений с помощью КТО для проверки навыков модульных вычислений.	ОПК-2.В.1

Перечень тем для выполнения курсового проекта/ курсовой работы представлены в таблице 17.

Таблица 17 – Перечень тем для выполнения курсового проекта / курсовой работы

№ п/п	Примерный перечень тем для выполнения курсового проекта/ курсовой работы
	Учебным планом не предусмотрено

Вопросы для проведения промежуточной аттестации в виде тестирования представлены в таблице 18.

Таблица 18 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов	Код индикатора
семестр 3		
1	Формула Байеса для вероятности гипотезы A при наблюдении B записывается как: A) $P(A \mid B) = \frac{P(B \mid A)}{P(B)}$ B) $P(A \mid B) = \frac{P(B \mid A) \cdot P(A)}{P(B)}$ C) $P(A \mid B) = \frac{P(A) \cdot P(B)}{P(B \mid A)}$ D) $P(A \mid B) = \frac{P(B)}{P(A \mid B)}$ Ответ: B	ПК-0.3.1, ПК-0.У.1, ПК-0.В.1
2	Какое из перечисленных свойств не является свойством энтропии Шеннона $H(X)$? A) $H(X) \geq 0$ B) $H(X) \leq \log_2 n$ (где n – число возможных значений) C) $H(X) = 0$, если распределение равномерное D) $H(X) = H(Y) + H(X \mid Y)$ для совместного распределения (цепное правило) Ответ: C (равномерное распределение даёт максимум, а не нуль)	ПК-0.3.1, ПК-0.У.1, ПК-0.В.1
3	Пропускная способность двоичного симметричного канала с вероятностью ошибки p равна: A) $C = 1 + p\log_2 p + (1-p)\log_2(1-p)$ B) $C = 1 - H(p)$, где $H(p)$ – энтропия двоичного источника C) $C = 1 - H_2(p)$, где $H_2(p) = -p\log_2 p - (1-p)\log_2(1-p)$ D) $C = \log_2(1 + \mathrm{SNR})$ Ответ: C	ПК-0.3.1, ПК-0.У.1, ПК-0.В.1
4	В конечном поле $GF(2^m)$ сложение выполняется как: A) Арифметическое сложение по модулю 2^m B) Побитовое исключающее ИЛИ (XOR) C) Сложение по модулю m D) Обычное сложение с переносом Ответ: B	ПК-0.3.1, ПК-0.У.1, ПК-0.В.1
5	Граница Хемминга для кода длины n, с числом информационных символов k и исправляющим t ошибок имеет вид: A) $2^k \cdot (1 + C(n,1) + \cdots + C(n,t)) \leq 2^n$ B) $2^k \geq \frac{2^n}{1+C(n,1)+\cdots+C(n,t)}$ C) $2^k \cdot (1 + C(n,1) + \cdots + C(n,t)) \geq 2^n$ D) $2^k \leq \frac{2^n}{1+C(n,1)+\cdots+C(n,2t)}$ Ответ: A	ПК-0.3.1, ПК-0.У.1, ПК-0.В.1
6	Какие из перечисленных мер являются аддитивными для независимых источников (событий)? (Отметьте все верные) A) Количество информации по Хартли B) Количество информации по Шеннону (энтропия) C) Собственная информация отдельного сообщения D) Взаимная информация $I(X;Y)$ Ответ: A, B, C	ПК-0.3.1, ПК-0.У.1, ПК-0.В.1
7	Какие утверждения о конечных полях верны? A) Поле $GF(p)$ существует для любого простого p B) Поле $GF(p^m)$ существует для любого простого p и любого натурального m C) Все ненулевые элементы поля образуют циклическую группу по умножению D) Характеристика поля $GF(2^m)$ равна 2^m Ответ: A, B, C (характеристика равна 2, а не 2^m)	ПК-0.3.1, ПК-0.У.1, ПК-0.В.1
8	Какие свойства относятся к проверочной матрице H линейного блочного кода? A) H имеет размерность $(n-k) \times n$ B) Синдром $s = H \cdot r^T$, где r – принятый вектор C) Все кодовые слова удовлетворяют $H \cdot c^T = 0$ D) H порождает код, а G его проверяет Ответ: A, B, C (D – наоборот)	ПК-0.3.1, ПК-0.У.1, ПК-0.В.1
9	Сопоставьте алгебраическую структуру с её определяющим свойством. Структура — Свойство 1. Группа — A) Абелева группа по сложению, ассоциативное умножение, дистрибутивность (часто с единицей) 2. Кольцо — B) Абелева группа по сложению и по умножению (без нуля), дистрибутивность 3. Поле — C) Множество с одной бинарной операцией: ассоциативность, нейтральный и обратный элементы 4. Векторное пространство — D) Множество с операциями сложения и умножения на скаляр, удовлетворяющее аксиомам Ответ: 1–C, 2–A, 3–B, 4–D.	ПК-0.3.1, ПК-0.У.1, ПК-0.В.1
10	Расположите распределения на множестве из 4 элементов в порядке возрастания энтропии $H(X)$: 1. Равномерное (все вероятности 1/4) 2. Вырожденное (одно событие с вероятностью 1) 3. Вероятности (0.5, 0.25, 0.125, 0.125) 4. Вероятности (0.4, 0.3, 0.2, 0.1) Правильный порядок (от наименьшей к наибольшей): 2, 3, 4, 1 (Значения: 0, ≈1.75, ≈1.846, 2 бит)	ПК-0.3.1, ПК-0.У.1, ПК-0.В.1
11	Установите правильную последовательность этапов работы с линейным кодом: 1. Выбор порождающей матрицы G 2. Определение проверочной матрицы H из условия $GH^T = 0$ 3. Кодирование информационного вектора u как $c = uG$ 4. Декодирование с помощью синдрома $s = Hr^T$ 5. Передача по каналу Правильный порядок: 1, 2, 3, 5, 4	ОПК-2.В.1, ОПК-2.У.1
12	Закончите предложение: Алгоритм Евклида для нахождения наибольшего общего делителя двух полиномов над полем заключается в последовательном делении с остатком, пока остаток не станет равным нулю. Последний ненулевой остаток является _____. Ответ: НОД (наибольшим общим делителем)	ПК-0.3.1, ПК-0.У.1, ПК-0.В.1
13	Верно ли утверждение: «Энтропия совместного распределения $H(X,Y)$ всегда больше или равна сумме энтропий $H(X) + H(Y)$»? Ответ: Неверно (на самом деле $H(X,Y) \leq H(X) + H(Y)$, равенство – при	ПК-0.3.1, ПК-0.У.1, ПК-0.В.1

	независимости)	
14	Верно ли утверждение: «В поле $GF(2)$ операция сложения эквивалентна логическому И (AND)»? Ответ: Неверно (сложение в $GF(2)$ – это XOR, а умножение – AND)	ПК-0.3.1, ПК-0.У.1, ПК-0.В.1
15	Верно ли утверждение: «Код Хемминга (7,4) может исправить все ошибки кратности 2 и менее»? Ответ: Неверно (он исправляет только одну ошибку, так как $d = 3$, $t = 1$)	ПК-0.3.1, ПК-0.У.1, ПК-0.В.1
16	Запишите формулу для собственной информации события, имеющего вероятность p. Ответ: $I(p) = -\log_2 p$ (или $\ln p$ в натуральных единицах)	ОПК-2.В.1, ОПК-2.У.1
	семестр 4	
1	Какая классификационная модель описывает связи между понятиями с помощью семантических отношений «род–вид», «часть–целое» и ассоциативных связей? A) Иерархическая B) Тезаурусная C) Алфавитно-предметная D) Фасетная Ответ: B	ПК-0.3.1
2	Какие из перечисленных утверждений о древовидных моделях верны? A) Каждый узел имеет не более одного родителя B) Дерево является частным случаем графа без циклов C) В дереве всегда есть корневой узел D) Дерево не может быть использовано для классификации Ответ: A,B,C	ПК-0.3.1
3	Сопоставьте модель классификации с её основным принципом: 1. Иерархическая 2. Тезаурусная 3. Алфавитно-предметная 4. Фасетная A) Разбиение по независимым признакам (фасетам) B) Семантические связи между понятиями C) Строгое подчинение уровней (родитель–потомок) D) Упорядочение по алфавиту или предметной области Ответ: 1–C, 2–B, 3–D, 4–A	ПК-0.3.1
4	Расположите шаги построения оптимального префиксного кода Хаффмана в правильной последовательности: 1. Строим бинарное дерево, объединяя два узла с наименьшими весами 2. Вычисляем частоты символов 3. Присваиваем коды, проходя от корня к листьям (0 – левый, 1 – правый) 4. Сортируем узлы по возрастанию весов Ответ: 2, 4, 1, 3	ПК-0.3.1
5	Вставьте пропущенное слово: «Основное преимущество кодов переменной длины перед кодами постоянной длины – это снижение _____ длины кодового слова при неравномерном распределении вероятностей символов». Ответ: средней (или «средней длины»)	ПК-0.3.1
6	Верно ли, что алгоритм Хаффмана гарантирует минимальную избыточность для любого заданного распределения вероятностей, даже если кодируются не отдельные символы, а блоки? ПК-0.3.1 Ответ: Неверно	ПК-0.3.1
7	Для алфавита с вероятностями {0,5; 0,25; 0,125; 0,125} постройте код Хаффмана и вычислите среднюю длину кода (в битах на символ). Запишите только число с точностью до двух знаков. Ответ: 1,75	ОПК-2.В.1
8	При каком распределении вероятностей кодирование постоянной длины становится столь же эффективным, как и переменной длины (по средней длине)? A) Равномерное B) Сильно неравномерное C) Экспоненциальное D) Нормальное Ответ: A	ОПК-2.У.1
9	Какие из перечисленных задач являются актуальными для криптографической защиты информации? A) Обеспечение конфиденциальности при передаче данных B) Защита от несанкционированного доступа к файлам C) Ускорение работы алгоритмов сжатия D) Аутентификация пользователей в системах Ответ: A, B, D	ПК-0.3.1, ПК-0.У.1
10	Сопоставьте компонент криптосистемы RSA с его назначением: 1. Открытая экспонента e 2. Закрытая экспонента d 3. Модуль n 4. Функция Эйлера $\varphi(n)$ A) Используется для расшифрования B) Используется для шифрования C) Определяет длину ключа D) Необходима для вычисления ключей Ответ: 1–B, 2–A, 3–C, 4–D	ПК-0.3.1

Перечень тем контрольных работ по дисциплине обучающихся заочной формы обучения, представлены в таблице 19.

Таблица 19 – Перечень контрольных работ

№ п/п	Перечень контрольных работ
	Не предусмотрено

12.4. Методические материалы, определяющие процедуры оценивания индикаторов, характеризующих этапы формирования компетенций, содержатся в локальных нормативных актах ГУАП, регламентирующих порядок и процедуру проведения текущего контроля успеваемости и промежуточной аттестации обучающихся ГУАП.

13. Методические указания для обучающихся по освоению дисциплины

13.1. Методические указания для обучающихся по прохождению практических занятий

Практическое занятие является одной из основных форм организации учебного процесса, заключающаяся в выполнении обучающимися под руководством преподавателя комплекса учебных заданий с целью усвоения научно-теоретических основ учебной дисциплины, приобретения умений и навыков, опыта творческой деятельности.

Целью практического занятия для обучающегося является привитие обучающимся умений и навыков практической деятельности по изучаемой дисциплине.

Планируемые результаты при освоении обучающимся практических занятий:

– закрепление, углубление, расширение и детализация знаний при решении конкретных задач;

– развитие познавательных способностей, самостоятельности мышления, творческой активности;

– овладение новыми методами и методиками изучения конкретной учебной дисциплины;

– выработка способности логического осмысления полученных знаний для выполнения заданий;

– обеспечение рационального сочетания коллективной и индивидуальной форм обучения.

Практические занятия начинаются с записи в журнал преподавателя присутствующих студентов. Затем объявляется тема практических занятий.

Преподаватель излагает краткий конспект необходимого теоретического материала. Затем он формулирует задачу и предлагает студентам самостоятельно ее решить. Выполнение задания проверяется в течении занятия преподавателем у каждого студента. Если студент самостоятельно правильно решил задачу, он получает максимум 5 баллов. Если студент решает задачу с помощью преподавателя, то получает максимум 4 балла. Затем, в конце семестра, оценки студентов (включая оценку посещаемости) переводятся в бонусы (качество) от 0 до 5 баллов. Эти бонусы добавляются к общей сумме баллов в рамках модульно-рейтинговой системы. Студентам выдается домашнее задание в виде задач, которые они сдают в установленные сроки

13.2. Методические указания для обучающихся по прохождению самостоятельной работы

В ходе выполнения самостоятельной работы, обучающийся выполняет работу по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

В процессе выполнения самостоятельной работы у обучающегося формируется целесообразное планирование рабочего времени, которое позволяет ему развивать умения и навыки в усвоении и систематизации приобретаемых знаний, обеспечивает высокий уровень успеваемости в период обучения, помогает получить навыки повышения профессионального уровня.

Методическими материалами, направляющими самостоятельную работу обучающихся, являются:

– учебно-методический материал по дисциплине.

13.3. Методические указания для обучающихся по прохождению текущего контроля успеваемости.

Текущий контроль успеваемости предусматривает контроль качества знаний обучающихся, осуществляемого в течение семестра с целью оценивания хода освоения дисциплины.

13.4. Методические указания для обучающихся по прохождению промежуточной аттестации.

Промежуточная аттестация обучающихся предусматривает оценивание промежуточных и окончательных результатов обучения по дисциплине. Она включает в себя:

– зачет – это форма оценки знаний, полученных обучающимся в ходе изучения учебной дисциплины в целом или промежуточная (по окончании семестра) оценка знаний обучающимся по отдельным разделам дисциплины с аттестационной оценкой «зачтено» или «не зачтено».

– дифференцированный зачет – это форма оценки знаний, полученных обучающимся при изучении дисциплины, при выполнении курсовых проектов, курсовых работ, научно-исследовательских работ и прохождении практик с аттестационной оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Лист внесения изменений в рабочую программу дисциплины

Дата внесения изменений и дополнений. Подпись внесшего изменения	Содержание изменений и дополнений	Дата и № протокола заседания кафедры	Подпись зав. кафедрой