

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
федеральное государственное автономное образовательное учреждение высшего образования  
"САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ"

Кафедра № 33

УТВЕРЖДАЮ

Руководитель направления

проф., д.т.н., доц.

(должность, уч. степень, звание)

С.В. Беззатеев

(инициалы, фамилия)



(подпись)

«25» мая 2023 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Алгоритмические проблемы криптографии»  
(Наименование дисциплины)

Код направления подготовки/ специальности	10.03.01
Наименование направления подготовки/ специальности	Информационная безопасность
Наименование направленности	Безопасность компьютерных систем
Форма обучения	очная

Санкт-Петербург– 2023



## Аннотация

Дисциплина «Алгоритмические проблемы криптографии» входит в образовательную программу высшего образования – программу бакалавриата по направлению подготовки/ специальности 10.03.01 «Информационная безопасность» направленности «Безопасность компьютерных систем». Дисциплина реализуется кафедрой «№33».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

ПК-1 «Способен определять состав программно-аппаратных средств защиты информации в операционных системах»

ПК-2 «Способен определять состав программно-аппаратных средств защиты информации в компьютерных сетях»

Содержание дисциплины охватывает круг вопросов, связанных с методами классической и современной алгебры и теории чисел, применяемых в криптографии, алгебраическими методами решения ряда основных задач, возникающих при синтезе криптографических алгоритмов.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, практические занятия, самостоятельная работа студентов.

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости, промежуточная аттестация в форме экзамена.

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

Содержание дисциплины охватывает круг вопросов, связанных с методами классической и современной алгебры и теории чисел, применяемых в криптографии, алгебраическими методами решения ряда основных задач, возникающих при синтезе криптографических алгоритмов.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, практические занятия, самостоятельная работа студентов.

1.2. Дисциплина входит в состав части, формируемой участниками образовательных отношений, 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
Профессиональные компетенции	ПК-1 Способен определять состав программно-аппаратных средств защиты информации в операционных системах	ПК-1.3.1 знает принципы функционирования средств защиты информации в операционных системах, в том числе использующих криптографические алгоритмы
Профессиональные компетенции	ПК-2 Способен определять состав программно-аппаратных средств защиты информации в компьютерных сетях	ПК-2.3.2 знает принципы функционирования сетевых протоколов, включающих криптографические алгоритмы ПК-2.У.1 умеет оценивать угрозы безопасности информации в компьютерных сетях

## 2. Место дисциплины в структуре ОП

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

- – «Математическая логика и теория алгоритмов»,
- – «Введение в направление»,
- – «Компьютерная алгебра»,
- – «Информатика».

Знания, полученные при изучении материала данной дисциплины, имеют как самостоятельное значение, так и могут использоваться при изучении других дисциплин:

- «Криптографические методы защиты информации»,
- – «Математические основы криптографии».

## 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
		№4
1	2	3
<b>Общая трудоемкость дисциплины, ЗЕ/ (час)</b>	4/ 144	4/ 144
<b>Из них часов практической подготовки</b>	34	34
<b>Аудиторные занятия, всего час.</b>	68	68
в том числе:		
лекции (Л), (час)	34	34
практические/семинарские занятия (ПЗ), (час)	17	17
лабораторные работы (ЛР), (час)		
курсовой проект (работа) (КП, КР), (час)	17	17
экзамен, (час)	36	36
<b>Самостоятельная работа, всего (час)</b>	40	40
<b>Вид промежуточной аттестации:</b> зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.**)	Экз.	Экз.

Примечание: \*\* кандидатский экзамен

#### 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 (час)	СРС (час)
Семестр 4					
Раздел 1. Элементы теории чисел	10	5			10
Раздел 2. Тесты простоты	6	6			10
Раздел 3. Задача факторизации составного числа	6	6			10
Раздел 4. Сложность вычислительных алгоритмов	12				10
Выполнение курсовой работы				17	
Итого в семестре:	34	17		17	40
Итого	34	17	0	17	40

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
<b>1</b>	Тема 1.1. Простые числа и "основная" теорема арифметики. Тема 1.2. Полная и приведенная системы вычетов. Тема 1.3. Теорема Эйлера и теорема Ферма. Тема 1.4. Алгоритм Евклида. Тема 1.5. Бинарный алгоритм возведения в степень. Тема 1.6. Китайская теорема об остатках.

	Тема 1.7. Квадратичные вычеты
2	Тема 2.1. Детерминистические тесты на простоту. Метод пробных делений. Критерий Вильсона. Тест Лукаса. Алгоритм Конягина-Померанса. Тема 2.2. Вероятностные тесты на простоту. Тест Соловья-Штрассена. Тест Рабина-Миллера. Тема 2.3. Построение больших простых чисел
3	Тема 3.1. (P-1)-метод Полларда. Ро-метод Полларда. Тема 3.2. Факторизация целых чисел с субэкспоненциальной сложностью. Тема 3.3. Факторизация чисел с помощью квадратичного решета.
4	Тема 4.1. Основные понятия теории сложности. Тема 4.2. Детерминированные машины Тьюринга и класс задач P. Тема 4.3. Недетерминированные алгоритмы и класс задач NP. Тема 4.4. Полиномиальная сводимость и NP-полные задачи. Тема 4.5. Методы теории сложности в криптографии.

#### 4.1. 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 4					
1	Элементы теории чисел	Решение задач	5	5	1
2	Тесты простоты	Решение задач	6	6	2
3	Задача факторизации составного числа	Решение задач	6	6	3
Всего			17	17	

#### 4.2. 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				

#### 4.3. Курсовое проектирование/ выполнение курсовой работы

Цель курсовой работы: изучение и реализация методов криптографической защиты информации в различных предметных областях.

Поставленная цель достигается путем решения следующих задач:

1. Обозначить сущность проблемы и рассмотреть задачи защиты информации в информационных и телекоммуникационных системах.
2. Установить угрозы информации и способы их воздействия на объекты защиты информации.
3. Рассмотреть методы и средства защиты информации.
4. Раскрыть концепцию информационной безопасности предприятия.
5. Реализовать алгоритмы криптографической защиты информации согласно выданному заданию.

Примерные темы заданий на курсовую работу приведены в разделе 10 РПД.

#### 4.4. 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 4, час
1	2	3
Изучение теоретического материала дисциплины (ТО)	20	20
Курсовое проектирование (КП, КР)		
Расчетно-графические задания (РГЗ)		
Выполнение реферата (Р)		
Подготовка к текущему контролю успеваемости (ТКУ)	10	10
Домашнее задание (ДЗ)		
Контрольные работы заочников (КРЗ)		
Подготовка к промежуточной аттестации (ПА)	10	10
Всего:	40	40

#### 5. Перечень учебно-методического обеспечения

для самостоятельной работы обучающихся по дисциплине (модулю)

Учебно-методические материалы для самостоятельной работы обучающихся указаны в п.п. 7-11.

#### 6. 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)
-----------------------	--------------------------	--

004 М 87	Организация безопасного доступа к информационным ресурсам [Текст]: учебное пособие / Н. Н. Мошак, Т. М. Татарникова; С.-Петербург. гос. ун-т аэрокосм. приборостроения. - СПб.: Изд-во ГУАП, 2014. - 121 с.	40
51(075) Б 93	Математическая логика [Текст]: учебное пособие / Д. В. Бутенина, В. М. Лагодинский; С.-Петербург. гос. ун-т аэрокосм. приборостроения. - СПб.: Изд-во ГУАП, 2011. - 52 с.	55
519.6/8 Л 17	Математические основы криптологии. Тесты простоты и факторизация [Текст]: учебное пособие / С. В. Лазарева, А. А. Овчинников; С.-Петербург. гос. акад. аэрокосм. приборостроения. - СПб.: Изд-во ГУАП, 2006. - 64 с.	79
519.7 Е 78	Элементы дискретной математики: учебное пособие/И. Л. Ерош, В. В. Михайлов; С.-Петербург. гос. ун-т аэрокосм. приборостроения. - СПб: ГОУ ВПО "СПбГУАП", 2008.	164
519.6/8 К53	Д. Кнут. Искусство программирования для ЭВМ. Т.2: Получисленные алгоритмы. М., Вильямс, 2005	22
004 К84	Крук Е.А., Линский Е.М. Криптография с открытым ключом. Кодовые системы. ГУАП, 2004.	20

1. Перечень электронных образовательных ресурсов 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
<a href="http://www.pgpru.com/">http://www.pgpru.com/</a>	Проект "OpenPGP в России"

2. Перечень информационных технологий

8.1. 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

8.2. 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

### 3. Материально-техническая база

Состав материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине, представлен в таблице 12.

Таблица 12 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы	Номер аудитории (при необходимости)
1	Фонд аудиторий ГУАП для проведения лекционных и семинарских (практических) занятий.	

### 7. Оценочные средства для проведения промежуточной аттестации

7.1. Состав оценочных средств для 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
Экзамен	Список вопросов к экзамену; Экзаменационные билеты; Задачи; Тесты.
Выполнение курсовой работы	Экспертная оценка на основе требований к содержанию курсовой работы по дисциплине.

7.2. 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	Характеристика сформированных компетенций
5-балльная шкала	
«отлично» «зачтено»	– обучающийся глубоко и всесторонне усвоил программный материал; – уверенно, логично, последовательно и грамотно его излагает; – опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью направления; – умело обосновывает и аргументирует выдвигаемые им идеи; – делает выводы и обобщения; – свободно владеет системой специализированных понятий.
«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.
«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;

Оценка компетенции	Характеристика сформированных компетенций
5-балльная шкала	
	<ul style="list-style-type: none"> <li>– слабо аргументирует научные положения;</li> <li>– затрудняется в формулировании выводов и обобщений;</li> <li>– частично владеет системой специализированных понятий.</li> </ul>
«неудовлетворительно» «не зачтено»	<ul style="list-style-type: none"> <li>– обучающийся не усвоил значительной части программного материала;</li> <li>– допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении;</li> <li>– испытывает трудности в практическом применении знаний;</li> <li>– не может аргументировать научные положения;</li> <li>– не формулирует выводов и обобщений.</li> </ul>

7.3. 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
1	Простые числа и "основная" теорема арифметики.	ПК-1.3.1
2	Полная и приведенная системы вычетов.	
3	Теорема Эйлера и теорема Ферма.	
4	Алгоритм Евклида.	
5	Бинарный алгоритм возведения в степень.	
6	Китайская теорема об остатках.	
7	Квадратичные вычеты	
8	Метод пробных делений.	
9	Критерий Вильсона.	
10	Тест Лукаса.	
11	Алгоритм Конягина-Померанса.	ПК-2.3.2
12	Детерминистические и вероятностные тесты на простоту.	
13	Тест Соловея-Штрассена.	
14	Тест Рабина-Миллера.	
15	Построение больших простых чисел	
16	Задача факторизации составного числа.	
17	(P-1)-метод Полларда.	
18	Po-метод Полларда.	
19	Факторизация чисел с помощью квадратичного решета.	
20	Основные понятия теории сложности.	
21	Детерминированные машины Тьюринга и класс задач P.	ПК-2.У.1
22	Недетерминированные алгоритмы и класс задач NP.	
23	Полиномиальная сводимость и NP-полные задачи.	
24	Методы теории сложности в криптографии.	

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
	Учебным планом не предусмотрено	

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

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

№ п/п	Примерный перечень тем для курсового проектирования/выполнения курсовой работы
	1. Самостоятельный анализ исторического шифра. Шифры простой

	<p>замены, Плейфера, Виженера, Полибия, Хилла, Вернама, «Решетка», Хейглина, Enigma и др.</p> <ol style="list-style-type: none"> <li>2. Режимы блочного шифрования ГОСТ 28147-89, DES.</li> <li>3. Алгоритм разворачивания ключа шифра AES.</li> <li>4. Исследование энтропийных свойств русского и английского языков.</li> <li>5. Генераторы ПСП и их свойства.</li> <li>6. Самосинхронизирующиеся поточные шифры.</li> <li>7. Построение чистого шифра. Оценка трудоемкости подбора ключа при известной паре «открытый – шифрованный текст».</li> <li>8. Теория имитостойкости Симмонса. Оценка вероятности имитации ключевых хэш-функций.</li> <li>9. Построение защитных контрольных сумм на основе бесключевой хэш-функции.</li> <li>10. Построение криптографической хэш-функции на основе односторонней функции.</li> <li>11. Построение класса больших простых чисел.</li> <li>12. Вероятностные тесты на простоту. Построение доказуемо простых чисел.</li> <li>13. Построение ключевой информации для ЭЦП.</li> <li>14. Вычисления на эллиптической кривой.</li> <li>15. Инфраструктура открытых ключей.</li> </ol>
--	--

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								
	<ul style="list-style-type: none"> <li>• В протоколе шифра Шамира сообщение пересылается               <ol style="list-style-type: none"> <li>а) два раза</li> <li>б) три раза</li> <li>в) один раз</li> <li>г) четыре раза.</li> </ol> </li> <li>• Надежность системы RSA базируется на том, что               <ol style="list-style-type: none"> <li>а) сложно определить по данному числу, является ли оно простым</li> <li>б) задача дискретного логарифмирования сложна</li> <li>в) задача разложения на множители числа, являющегося произведением двух простых, сложна.</li> </ol> </li> <li>• Укажите правильный порядок ответов в правом столбике:               <table style="width: 100%; border: none;"> <tr> <td style="width: 50%;">RC4</td> <td>шифр с открытым ключом</td> </tr> <tr> <td>AES</td> <td>поточковый шифр</td> </tr> <tr> <td>RSA</td> <td>совершенный шифр</td> </tr> <tr> <td>Шифр Вернама</td> <td>блоковый шифр</td> </tr> </table> </li> </ul>	RC4	шифр с открытым ключом	AES	поточковый шифр	RSA	совершенный шифр	Шифр Вернама	блоковый шифр	
RC4	шифр с открытым ключом									
AES	поточковый шифр									
RSA	совершенный шифр									
Шифр Вернама	блоковый шифр									

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

7.4. 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.

#### 4. Методические указания для обучающихся по освоению дисциплины

Целью дисциплины является – получение студентами необходимых знаний, умений и навыков в области алгебраических методов криптографии, создание поддерживающей образовательной среды преподавания криптографических методов и средств защиты информации, предоставление возможности студентам развить и продемонстрировать навыки в области дискретной математики, компьютерной алгебры и алгебраической алгоритмики.

11.1. Методические указания для обучающихся по освоению лекционного материала.

Основное назначение лекционного материала – логически стройное, системное, глубокое и ясное изложение учебного материала. Назначение современной лекции в рамках дисциплины не в том, чтобы получить всю информацию по теме, а в освоении фундаментальных проблем дисциплины, методов научного познания, новейших достижений научной мысли. В учебном процессе лекция выполняет методологическую, организационную и информационную функции. Лекция раскрывает понятийный аппарат конкретной области знания, её проблемы, дает цельное представление о дисциплине, показывает взаимосвязь с другими дисциплинами.

Планируемые результаты при освоении обучающимися лекционного материала:

- получение современных, целостных, взаимосвязанных знаний, уровень которых определяется целевой установкой к каждой конкретной теме;
- получение опыта творческой работы совместно с преподавателем;
- развитие профессионально-деловых качеств, любви к предмету и самостоятельного творческого мышления.

- появление необходимого интереса, необходимого для самостоятельной работы;
- получение знаний о современном уровне развития науки и техники и о прогнозе их развития на ближайшие годы;
- научиться методически обрабатывать материал (выделять главные мысли и положения, приходиться к конкретным выводам, повторять их в различных формулировках);
- получение точного понимания всех необходимых терминов и понятий.

Лекционный материал может сопровождаться демонстрацией слайдов и использованием раздаточного материала при проведении коротких дискуссий об особенностях применения отдельных тематик по дисциплине.

#### Структура предоставления лекционного материала:

Раздел 1. Элементы теории чисел

Тема 1.1. Простые числа и "основная" теорема арифметики. Тема 1.2. Полная и приведенная системы вычетов.

Тема 1.3. Теорема Эйлера и теорема Ферма. Тема 1.4. Алгоритм Евклида.

Тема 1.5. Бинарный алгоритм возведения в степень. Тема 1.6. Китайская теорема об остатках.

Тема 1.7. Квадратичные вычеты

Раздел 2. Тесты простоты

Тема 2.1. Детерминистические тесты на простоту. Метод пробных делений.

Критерий Вильсона. Тест Лукаса. Алгоритм Конягина Померанса.

Тема 2.2. Вероятностные тесты на простоту. Тест Соловья-Штрассена. Тест Рабина-Миллера.

Тема 2.3. Построение больших простых чисел

Раздел 3. Задача факторизации составного числа. Тема 3.1. (P-1)-метод Полларда. Ро-метод Полларда.

Тема 3.2. Факторизация целых чисел с субэкспоненциальной сложностью. Тема

3.3. Факторизация чисел с помощью квадратичного решета

Раздел 4. Сложность вычислительных алгоритмов

Тема 4.1. Основные понятия теории сложности.

Тема 4.2. Детерминированные машины Тьюринга и класс задач P. Тема 4.3.

Недетерминированные алгоритмы и класс задач NP. Тема 4.4. Полиномиальная сводимость и NP-полные задачи.

Тема 4.5. Методы теории сложности в криптографии.

11.2. Методические указания для обучающихся по участию в семинарах  
Учебным планом не предусмотрено.

11.3. 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.

#### Требования к проведению практических занятий

Практические занятия проводятся в виде разбора и решения задач. По каждой теме предусмотрено выполнение ряда задач. Контроль и закрепление знаний по каждой теме осуществляется в виде опроса у доски, аудиторных контрольных работ и домашних заданий.

11.4. Методические указания для обучающихся по выполнению лабораторных работ

Учебным планом не предусмотрено.

11.5. Методические указания для обучающихся по прохождению курсового проектирования/выполнения курсовой работы

Курсовой проект/ работа проводится с целью формирования у обучающихся опыта комплексного решения конкретных задач профессиональной деятельности.

Курсовой проект/ работа позволяет обучающемуся:

- систематизировать и закрепить полученные теоретические знания и практические умения по профессиональным учебным дисциплинам и модулям в соответствии с требованиями к уровню подготовки, установленными программой учебной дисциплины, программой подготовки специалиста соответствующего уровня, квалификации;

- применить полученные знания, умения и практический опыт при решении комплексных задач, в соответствии с основными видами профессиональной деятельности по направлению/ специальности/ программе;

- углубить теоретические знания в соответствии с заданной темой;

- сформировать умения применять теоретические знания при решении нестандартных задач;

- приобрести опыт аналитической, расчётной, конструкторской работы и сформировать соответствующие умения;

- сформировать умения работы со специальной литературой, справочной, нормативной и правовой документацией и иными информационными источниками;

- сформировать умения формулировать логически обоснованные выводы, предложения и рекомендации по результатам выполнения работы;

- развить профессиональную письменную и устную речь обучающегося;

- развить системное мышление, творческую инициативу, самостоятельность, организованность и ответственность за принимаемые решения;

- сформировать навыки планомерной регулярной работы над решением поставленных задач.

#### **Структура пояснительной записки курсовой работы / проекта**

Изучение курса «Управление данными» заканчивается выполнением курсовой работы по проектированию баз данных различного назначения. Содержание курсового проекта излагается в программе курса для соответствующих специальностей и должно соответствовать приведенному в приложении заданию на курсовое проектирование. Бланк задания на курсовое проектирование должен быть подшит в пояснительную записку перед введением.

Отчёт по курсовой работе оформляется каждым студентом индивидуально и содержит описание лично выполненной работы, которая включает:

- титульный лист;
- индивидуальное задание;
- пояснительную записку;
- программы и спецификации на электронном носителе;

Пояснительная записка содержит разделы:

- содержание с указанием страниц и разделов;
- введение;
- основную часть;
- список литературы;
- приложения.

В содержании должна быть отражена структура пояснительной записки. Введение должно характеризовать ту сферу человеческой деятельности, для которой будет проектироваться приложение.

Список литературы, помимо книг, использованных при работе над курсовой работой, должен включать ссылки на все электронные материалы, использованные при проектировании.

Листинги программ с подробными комментариями должны быть приведены в приложениях.

### **Требования к оформлению пояснительной записки курсовой работы / проекта**

В виду принадлежности курсового проекта к дисциплинам связанным с информационными технологиями и электронно-вычислительными машинами пояснительная записка должна быть оформлена при помощи любого программного инструмента и распечатана на листах формата А4 (210×297 мм), листы должны быть пронумерованы и сшиты. Поля листа должны составлять левое 25 мм, верхнее и нижнее 20 мм, правое 15 мм. Текст записки должен быть набран удобочитаемым шрифтом по размеру и начертанию соответствующий «Times New Roman» в 14 пт. Межстрочный интервал должен соответствовать полуторному. В записке также должен быть предусмотрен карман для помещения в него диска с работоспособным приложением и всеми исходными текстами программ. Допускается помещать на дискету архив в формате zip или rar.

Полный листинг программы должен включать в себя распечатку всех файлов программ, из которых состоит проект. Формы проекта должны быть распечатаны в двух видах: в виде формы и в виде тестового файла. Все файлы форм должны быть сгруппированы в следующей последовательности: сначала форма в процессе разработки, затем форма в текстовом виде и в завершении текст модуля связанный с формой. В записке фрагменты текстов программы, а также тексты распечаток модуля и формы должны быть выполнены шрифтом «Courier New» размером 10 пт., через одинарный интервал.

#### **11.6. 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 им 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.

#### **11.7. 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. Форма проведения текущего контроля – защита отчетов по лабораторным работам. Результаты текущего контроля учитываются при проведении промежуточной аттестации в соответствии с требованиями СТО ГУАП. СМК 3.76 «Положение о текущем контроле успеваемости и промежуточной аттестации студентов и аспирантов ГУАП, обучающихся по образовательным программам высшего образования».

#### **11.8. Методические указания для обучающихся по прохождению промежуточной аттестации.**

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

Экзамен – форма оценки знаний, полученных обучающимся в процессе изучения всей дисциплины или ее части, навыков самостоятельной работы, способности применять их для решения практических задач. Экзамен, как правило, проводится в период экзаменационной сессии и завершается аттестационной оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Система оценок при проведении промежуточной аттестации осуществляется в соответствии с требованиями Положений «О текущем контроле успеваемости и промежуточной аттестации студентов ГУАП, обучающихся по программы высшего образования» и «О модульно-рейтинговой системе оценки качества учебной работы студентов в ГУАП».

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