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

Кафедра № 33

УТВЕРЖДАЮ
Ответственный за образовательную программу

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

Т.Н. Елина
(инициалы, фамилия)

(подпись)
«27» июня 2024 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
Год приема	2024

Санкт-Петербург– 2024

Лист согласования рабочей программы дисциплины

Программу составил (а)

доц.,к.э.н.,доц. (должность, уч. степень, звание) | 27.06.2024 (подпись, дата) | Т.Н. Елина (инициалы, фамилия)

Программа одобрена на заседании кафедры № 33
«27» июня 2024 г, протокол № 11

Заведующий кафедрой № 33

д.т.н.,доц. (уч. степень, звание) | 27.06.2024 (подпись, дата) | С.В. Беззатеев (инициалы, фамилия)

Заместитель директора института №3 по методической работе

(должность, уч. степень, звание) | 27.06.2024 (подпись, дата) | Н.В. Решетникова (инициалы, фамилия)

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.З.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.З.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
Общая трудоемкость дисциплины, ЗЕ/ (час)	4/ 144	4/ 144
Из них часов практической подготовки	34	34
Аудиторные занятия, всего час.	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
Самостоятельная работа, всего (час)	40	40
***Вид промежуточной аттестации*:** зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.**)	Экз.	Экз.

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			5
Раздел 2. Тесты простоты	6	6			5
Раздел 3. Задача факторизации составного числа	6	6			5
Раздел 4. Сложность вычислительных алгоритмов	12				6
Итого в семестре:	34	17			21
Итого	34	17	0	17	21

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

1	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. АлгоритмКонягина-Померанса. Тема 2.2. Вероятностные тесты на простоту. Тест Соловея-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 субэкспоненциальнойсложностью. Тема 3.3. Факторизация чисел с помощью квадратичногорешета.
4	Тема 4.1. Основные понятия теории сложности. Тема 4.2. Детерминированные машины Тьюринга и классзадач 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.

4.3. 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 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	

4.4. 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. Курсовое проектирование/ выполнение курсовой работы

Цель курсовой работы: Изучение, освоение и реализация криптографических алгоритмов

Часов практической подготовки: 17

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

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 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.-Петерб. 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.-Петерб. гос. ун-т аэрокосм. приборостроения. - СПб.: Изд-во ГУАП, 2011. - 52 с.	55
519.6/.8	Математические основы криптологии.	79

Л 17	Тесты простоты и факторизация [Текст]: учебное пособие / С. В. Лазарева, А. А. Овчинников; С.-Петерб. гос. акад. аэрокосм. приборостроения. - СПб.: Изд-во ГУАП, 2006. - 64 с.	
519.7 Е 78	Элементы дискретной математики: учебное пособие/И. Л. Ерош, В. В. Михайлов; С.- Петерб. 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

7. 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
http://www.pgpru.com/	Проект "OpenPGP в России"

8. 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

9. 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	Лекционная аудитория	
2	Мультимедийная лекционная аудитория	

10. Оценочные средства для проведения промежуточной аттестации

10.1. 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
Экзамен	Список вопросов к экзамену; Экзаменационные билеты; Задачи; Тесты.
Выполнение курсовой работы	Экспертная оценка на основе требований к содержанию курсовой работы по дисциплине.

10.2. 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 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 5-балльная шкала	Характеристика сформированных компетенций
	– слабо аргументирует научные положения; – затрудняется в формулировании выводов и обобщений; – частично владеет системой специализированных понятий.
«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.

10.3. 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. Полная и приведенная системы вычетов. Теорема Эйлера и теорема Ферма. Алгоритм Евклида. Бинарный алгоритм возведения в степень. Китайская теорема об остатках.	ПК-1.З.1
2	Квадратичные вычеты Метод пробных делений. Критерий Вильсона. Тест Лукаса. Алгоритм Конягина-Померанса. Детерминистические и вероятностные тесты на простоту. Тест Соловея-Штрассена. Тест Рабина-Миллера. Построение больших простых чисел Задача факторизации составного числа.	ПК-2.З.2
3	(P-1)-метод Полларда. Ро-метод Полларда. Факторизация чисел с помощью квадратичного решета. Основные понятия теории сложности. Детерминированные машины Тьюринга и класс задач P. Недетерминированные алгоритмы и класс задач NP. Полиномиальная сводимость и NP-полные задачи. Методы теории сложности в криптографии.	ПК-2.У.1

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. Разработка программного обеспечения, реализующего криптозащиту данных с использованием нескольких методов. 2. Проведение анализа применения блочных криптосистем в системе защиты информации предприятия. 3. Применение алгоритмов электронной цифровой подписи в автоматизированной системе управления делопроизводством. 4. Проведение сравнительного анализа эффективности современных программных, программно-аппаратных и аппаратных средств криптографической защиты. 5. Оценка эффективности криптографических генераторов, основанных на алгоритмах Фибоначчи. 6. Проведение сравнительного анализа алгоритмов формирования хэш-функций. 7. Исследование практического применения криптографических протоколов распределения ключей. 8. Разработка системы аутентификации сотрудников производственного предприятия.

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
	1. Наука, занимающаяся проблемой защиты информации путем ее преобразования - это A. криптология B. криптография C. криптоанализ D. шифрование 2. Наука, занимающаяся исследованием возможности расшифровывания информации без знания ключей - это A. криптоанализ B. криптология C. криптография D. шифрование 3. Конечное множество используемых для кодирования информации знаков - это A. алфавит	

B. текст
C. шифр
D. ключ

4. Преобразовательный процесс, при котором исходный текст заменяется шифрованным текстом - это

A. шифрование
B. дешифрование
C. декодирование
D. кодирование

5. Преобразовательный процесс, при котором шифрованный текст преобразуется в исходный - это

A. дешифрование
B. шифрование
C. кодирование
D. декодирование

6. Информация, необходимая для беспрепятственного шифрования и дешифрирования текстов - это

A. ключ
B. алфавит
C. шифр
D. код

7. Из перечисленных: 1) симметричные, 2) несимметричные, 3) с открытым ключом, 4) с закрытым ключом - различают криптосистемы

A. 1, 3
B. 1, 2
C. 3, 4
D. 1, 4

8. Криптосистемы, в которых для шифрования и для дешифрования используется один и тот же ключ называются криптосистемами

A. симметричными
B. несимметричными
C. с открытым ключом
D. с закрытым ключом

9. Криптосистемы, в которых ннформация шифруется с помощью одного ключа, а расшифровывается с помощью другого ключа, известного только получателю сообщения называются криптосистемами

A. с открытым ключом

B. с закрытым ключом
C. симметричными
D. несимметричными

10. В криптосистемах с открытым ключом

A. открытый ключ доступен всем желающим, закрытый ключ доступен только получателю сообщения
B. для шифрования и дешифрования используется один ключ
C. закрытый ключ доступен всем желающим, открытый ключ доступен только получателю сообщения
D. закрытый и открытый ключи доступны всем желающим

11. Присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения, называется

A. электронной подписью
B. идентификатором
C. ключом
D. шифром

12. Характеристика шифра, определяющая стойкость шифра к дешифрованию без знания ключа, называется

A. криптостойкостью
B. надежностью
C. эффективностью
D. уровнем безопасности

13. Из перечисленных: 1) количество всех возможных ключей, 2) размер алфавита, 3) размер открытого текста, 4) среднее время криптоанализа - к показателям криптостойкости шифра относятся

A. 1, 4
B. 1, 2, 3, 4
C. 2, 3
D. 1, 2, 3

14. Из перечисленных: 1) замена, 2) перестановка, 3) гаммирование, 4) смысловое кодирование, 5) рассечение и разнесение - к методам шифрования информации относятся

A. 1, 2, 3
B. 1, 2, 3, 4, 5
C. 4, 5
D. 1, 2, 3, 4

15. Из перечисленных: 1) одноалфавитная, 2) многоалфавитная, 3) смысловая, 4) механическая - к методам шифрования

информации способом замены относятся

A. 1, 2
B. 1, 2, 3, 4
C. 3, 4
D. 1, 2, 3

16. Из перечисленных: 1) простая, 2) усложненная по таблице, 3) усложненная по маршрутам, 4) одноалфавитная, 5) многоалфавитная - к методам шифрования информации способом перестановки относятся

A. 1, 2, 3
B. 1, 2, 3, 4, 5
C. 4, 5
D. 2, 3, 4, 5

17. Шифрование - это вид криптографического закрытия,

A. при котором преобразованию подвергается каждый символ защищаемого сообщения
B. при котором преобразованию подвергается сообщение целиком, но не каждый его символ
C. при котором к каждому символу приписывается кодовая комбинация
D. который обеспечивает невозможность расшифровки

18. Кодирование - это вид криптографического закрытия,

A. при котором некоторые элементы защищаемых данных (это не обязательно отдельные символы) заменяются заранее выбранными кодами
B. при котором каждый символ защищаемых данных заменяется заранее выбранным кодом
C. при котором к каждому символу приписывается кодовая комбинация
D. который обеспечивает полную невозможность чтения сообщения

19. Шифр, который производит замену каждой буквы открытого текста на символ шифрованного текста, называется

A. подстановка
B. перестановка
C. гаммирование
D. блочный

20. Шифр, у которого буквы открытого текста не замещаются на другие, а меняется порядок их следования, называется

A. перестановка
B. подстановка

C. гаммирование
D. блочный

21. Шифр, который заключается в наложении на исходный текст некоторой псевдослучайной последовательности, генерируемой на основе ключа, называется

A. гаммирование
B. перестановка
C. подстановка
D. блочный

22. Шифр, который представляет собой последовательность (с возможным повторением и чередованием) основных методов преобразования, применяемую к части шифруемого текста, называется

A. блочный
B. рассечение-разнесение
C. подстановка
D. гаммирование

23. Шифр, который заключается в том, что массив защищаемых данных делится на такие элементы, каждый из которых в отдельности не позволяет раскрыть содержание защищаемой информации, и которые хранятся по разным зонам ЗУ или располагаются на различных носителях, называется

A. рассечение-разнесение
B. блочный
C. гаммирование
D. перестановка

24. Из перечисленных: 1) смысловое, 2) символьное, 3) блочное, 4) гаммирование - к методам криптографического закрытия информации способом кодирования относятся

A. 1, 2
B. 1, 2, 3, 4
C. 3, 4
D. 1, 2, 4

25. При символьном кодировании

A. кодируется каждый символ защищаемого сообщения
B. символы защищаемого сообщения меняются местами в соответствии с днем недели
C. закодированное сообщение имеет вполне определенный смысл (слова, предложения, группы предложений)
D. символы защищаемого сообщения меняются местами случайным образом

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

10.4. 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.

11. Методические указания для обучающихся по освоению дисциплины

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, приходить 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:

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 Соловея-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 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 тема осуществляется в виде опроса у доски, аудиторных контрольных работ и домашних заданий.

11.3. 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: осваивать основные алгоритмы криптографии с помощью практический реализации в виде программных продуктов

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 курсового проекта/ работы

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 курсового проекта/ работы

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.

11.4. 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.

Для обучающихся по заочной форме обучения, самостоятельная работа может включать в себя контрольную работу.

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 обучающихсяявляются:

- учебно-методический материал по дисциплине;
- методические указания по выполнению контрольных работ (для обучающихся по заочной форме обучения).

11.5. 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.

11.6. 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».

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