МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Чувашский государственный университет имени И. Н. Ульянова»

Факультет информатики и вычислительной техники

Кафедра математического и аппаратного обеспечения информационных систем

«УТВЕРЖДАЮ»
Проректор по учебной работе

_____ И.Е. Поверинов

31 августа 2017 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Математические основы криптологии»

Направление подготовки (специальность) – 10.05.03 «Информационная безопасность автоматизированных систем»

Квалификация (степень) выпускника – Специалист по защите информации

Специализация – «Безопасность открытых информационных систем»

Чебоксары – 2017

Рабочая программа основана на требованиях Федерального государственного образовательного стандарта высшего образования по специальности 10.05.03 «Информационная безопасность автоматизированных систем», утвержденного приказом Министерства образования и науки 01.12.2016 г. №1509

СОСТАВИТЕЛЬ (СОСТАВИТЕЛИ):

Кандидат физико-математических наук, доцент _____ С.В. Сейфуллина

ОБСУЖДЕНО:
на заседании кафедры МиАОИС 30 «августа» 2017 г., протокол № 1

заведующий кафедрой _____ Д. В. Ильин

СОГЛАСОВАНО:

Методическая комиссия ИВТ 30 «августа» 2017 г., протокол № 1

Декан факультета _____ А. В. Щипцова

Директор научной библиотеки _____ Н. Д. Никитина

Начальник управления информатизации _____ И. П. Пивоваров

Начальник учебно-методического управления _____ В. И. Маколов

Оглавление

1. Цель и задачи обучения по дисциплине

Цель - научить специалиста в области защиты информации основным алгоритмам теории чисел и арифметики многократной точности, используемым в программных и аппаратных реализациях криптографических систем.

Основными задачами дисциплины являются:

– формирование знаний о фундаментальных математических основах построения криптосистем;

– выработка знаний и умений разбираться в закономерностях, создания, использования и анализа современных криптосистем;

– выработка знаний и умений применять полученные теоретические сведения для решения практических задач.

2. Место дисциплины в структуре основной образовательной программы (ООП)

Дисциплина относится к дисциплинам базовой части образовательной программы по специальности 10.05.03 Информационная безопасность автоматизированных систем. Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин: Алгебра и геометрия, Математический анализ, Информатика, Языки программирования.

Дисциплина является предшествующей для дисциплин: Управление информационной безопасностью, Криптографические методы защиты информации, Криптографические протоколы и стандарты, прохождения практик, государственной итоговой аттестации.

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ООП

Процесс обучения по дисциплине направлен на формирование следующих компетенций:

способность корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники (ОПК-2).

В результате обучения по дисциплине, обучающийся должен (ЗУН):

знать:

криптологическую терминологию (З1);

основные теоремы теории чисел, используемые в криптологии (З2);

основные теоретико-числовые алгоритмы (З3);

основные алгоритмы, реализующие арифметические операции в основных алгебраических структурах, используемых в криптографических приложениях (З4);

взаимосвязь математических параметров и основные требования к ним в современных криптосистемах (З5);

уметь:

реализовывать основные теоретико-числовые и получисленные алгоритмы в криптографических приложениях (У1);

выполнять построение криптосистем на основе готовых криптографических библиотек (У2);

проводить математическое моделирование в криптологии (У3);

приводить математическое доказательство работоспособности предложенной криптосистемы (У4);

пользоваться современной научно-технической литературой в области криптологии (У5);

владеть навыками:

применения математического аппарата при решении профессиональных задач (Н1);

современными алгоритмами криптоанализа ассиметричных криптосистем (Н2).

4. Структура и содержание дисциплины

Образовательная деятельность по дисциплине проводится:

– в форме контактной работы обучающихся с педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях (далее – контактная работа);

– в форме самостоятельной работы.

Контактная работа включает в себя занятия лекционного типа, занятия семинарского типа (семинары, практические занятия, практикумы), групповые и (или) индивидуальные консультации, в том числе в электронной информационно-образовательной среде.

Обозначения:

Л – лекции, п/р – практические занятия, КСР – контроль самостоятельной работы, СРС – самостоятельная работа студента, ИФР – интерактивная форма работы.

4.1. Содержание дисциплины

Содержание	Формируемые компетенции	Формируемые ЗУН
Введение Тема 1. История математических моделей шифров. Основные алгебраические структуры в криптологии Тема 2. Анализ простейших шифров. Решение сравнений. Квадратичные вычеты. Поля Галуа. Тема 3. Основы теории непрерывных дробей Тема 4. Арифметические операции над целыми числами и многочленами Тема 5. Проверка чисел на простоту Тема 6. Факторизация чисел Тема 7. Дискретное логарифмирование в конечном поле Тема 8. Элементы теории решеток Тема 9. Элементы теории эллиптических кривых	ОПК-2	З1-З5, У1-У5, Н1-Н2
Зачет	ОПК-2	З1-З5, У1-У5, Н1-Н2

4.2. Объем дисциплины, виды учебной работы обучающихся по очной форме обучения

Содержание	Всего, час	Контактная работа, час			СРС, час	ИФР, час
		Л	п/р	КСР		
Введение	4	2			2	
Тема 1. История математических моделей шифров. Основные алгебраические структуры в криптологии	8	2	4		2	2
Тема 2. Анализ простейших шифров. Решение сравнений. Квадратичные вычеты. Поля Галуа.	10	2	4		4	4
Тема 3. Основы теории непрерывных дробей	6	2			4	
Тема 4. Арифметические операции над целыми числами и многочленами	13	4	4		5	4
Тема 5. Проверка чисел на простоту	13	4	4		5	4
Тема 6. Факторизация чисел	13	4	4		5	4
Тема 7. Дискретное логарифмирование в конечном поле	13	4	4		5	4
Тема 8. Элементы теории решеток	12	4	4		4	4
Тема 9. Элементы теории эллиптических кривых	12	4	4		4	4
Зачет	2			2	2	
Итого	**108 3 з.е.**	**32**	**32**	**2**	**42**	**30**

5. Содержание разделов дисциплины

5.1. Лекции и практические занятия

Введение

Обзор разделов математической науки, результаты которых использует криптология. Логическое построение курса.

Тема 1. История математических моделей шифров. Основные алгебраические структуры в криптологии

Свойства операций. Понятие алгебраической структуры. Понятие группы. Математическое моделирование шифра Цезаря. Понятие кольца. Математическое моделирование аффинного шифра. Делимость в кольце целых чисел. Наибольший общий делитель и наименьшее общее кратное. Алгоритм Евклида. Функция Эйлера. Бинарный и расширенный алгоритмы Евклида. Простые числа и их свойства. Распределение простых чисел. Понятие простого конечного поля.

Тема 2. Анализ простейших шифров. Решение сравнений. Квадратичные вычеты. Поля Галуа

Отношение сравнимости. Сравнения первой степени и их решение. Китайская теорема об остатках. Сравнения второй степени. Символы Лежандра и Якоби. Извлечение квадратного корня по модулю простого числа. Алгоритм Шенкса. Модульное возведение в степень. Малая теорема Ферма. Обобщение Эйлера для малой теоремы Ферма. Задача RSA. Протокол Диффи-Хеллмана. Криптосистема Эль-Гамаля. Простейшая арифметика в кольце многочленов. Алгоритм Евклида для многочленов. Теорема Лагранжа. Поля Галуа. Характеристика поля. Поле разложения многочлена. Решение систем линейных уравнений над конечным полем. Неприводимые многочлены.

Тема 3. Основы теории непрерывных дробей.

Определение непрерывной дроби. Подходящие дроби. Квадратичные иррациональности. Непрерывные дроби в решении задач. Простейшие Диофантовы уравнения. Уравнение Пелля. Представление числа в виде суммы квадратов. Разложение функций в непрерывные дроби.

Тема 4. Арифметические операции над целыми числами и многочленами.

Сложение и вычитание. Умножение в столбик. Возведение в квадрат. Умножение методом Карацубы-Оффмана. Умножение в классах вычетов. Дискретное преобразование Фурье. Умножение с помощью быстрого преобразования Фурье. Алгоритм Шенхаге-Штрассена. Модульное умножение. Метод Монтгомери. Модульное возведение в степень. Потенцирование методом «разделяй и властвуй». Параллельное потенцирование и умножение. Целочисленное деление с остатком. Приведение по модулю.

Тема 5. Проверка чисел на простоту

Решето Эратосфена. Вероятностные алгоритмы проверки чисел по на простоту. Тест Ферма. Тест Соловэя-Штрассена. Тест Миллера-Рабина. Генарация простого числа. Детерминированные алгоритмы проверки чисел на простоту. Тестирование и поиск неприводимых многочленов. Ассимптотически быстрые и вероятностные тесты многочленов на неприводимость.

Тема 6. Факторизация чисел

Пробное деление. Ро-методы Полларда. Метод квадратов. Метод непрерывных дробей. Метод квадратичного решета.

Тема 7. Дискретное логарифмирование в конечном поле.

Задача дискретного логарифмирования. Ро-метод Полларда. Методы Гельфонда и Сильвера-Полига-Хеллмана. Метод встречи посередине. Метод базы разложения.

Тема 8. Элементы теории решеток

Процесс ортогонализации Грама-Шмидта. Алгоритм Ленстры-Ленстры-Ловаша и его применение. Задача об укладке ранца. Ранцевые алгоритмы шифрования.

Тема 9. Элементы теории эллиптических кривых

Алгебраические кривые и эллиптические кривые. Однородное уравнение Вейерштрасса. Группа точек эллиптической кривой. Аномальные и суперсингулярные кривые. Групповой закон. Порядок эллиптической кривой над конечным полем. Теорема Хассе. Скалярное умножение. Примеры криптосистем

Практические занятия

1. Вычисление наибольшего общего делителя (4 ч., тема № 1).

2. Ассиметричные протоколы и криптосистемы (4 ч., тема №2)
3. Арифметические алгоритмы многократной точности для целых чисел и многочленов (4 ч, тема 4).
4. Вероятностные алгоритмы проверки чисел на простоту (4 ч, тема № 5).
5. Разложение чисел на множители (4 ч, тема № 6).
6. Дискретное логарифмирование в конечном поле. (4 ч, тема № 7).
7. Алгоритм Ленстры-Ленстры-Ловаша (4 ч., тема № 8).
8. Групповой закон и параметры криптосистем на основе эллиптических кривых. (4 ч, тема № 9).

5.2. Вопросы для самостоятельной работы студента.

1. Оптимальные базисы.
2. Схема Горнера.
3. Взаимосвязь компонентов RSA.
4. Криптосистемы

6. Образовательные технологии

В соответствии со структурой образовательного процесса по дисциплине применяются следующие технологии:

– применения знаний на практике, поиска новой учебной информации;
– организации совместной и самостоятельной деятельности обучающихся;

В соответствии с требованиями ФГОС ВО для реализации компетентностного подхода при обучении дисциплине предусмотрено широкое использование в учебном процессе активных и интерактивных методов проведения занятий:

При обучении дисциплине применяются следующие формы занятий:

– лекции, направленные на получение новых и углубление научно-теоретических знаний, в том числе вводная лекция, информационная лекция, обзорная лекция, лекция-консультация, проблемная лекция, лекции-дискуссии, лекции-беседы и др.;
– практические занятия, проводимые под руководством преподавателя в учебной аудитории, направленные на углубление и овладение определенными методами самостоятельной работы, могут включать коллективное обсуждение материала, дискуссии, решение и разбор конкретных практических ситуаций, компьютерные симуляции, тренинги и др.;

Все занятия обеспечены мультимедийными средствами (SMART доски, проекторы, экраны) для повышения качества восприятия изучаемого материала. В образовательном процессе широко используются информационно-коммуникационные технологии.

Самостоятельная работа студентов – это планируемая работа студентов, выполняемая по заданию при методическом руководстве преподавателя, но без его непосредственного участия. Формы самостоятельной работы студентов определяются содержанием учебной дисциплины, степенью подготовленности студентов. Они могут иметь учебный или учебно-исследовательский характер: аннотирование и конспектирование литературы по теме, составление вопросов и тестов к теме.

Формами контроля самостоятельной работы выступают оценивание устного выступления студента на практическом занятии, его доклада; проверка письменных отчётов по результатам выполненных заданий. Результаты самостоятельной работы учитываются при оценке знаний на зачёте.

7. Формы аттестации и оценочные материалы

Текущий контроль предназначен для проверки хода и качества усвоения учебного материала, стимулирования учебной работы обучающихся и совершенствования методики проведения занятий. Он проводится в ходе всех видов занятий в форме, избранной преподавателем.

Промежуточная аттестация имеет целью определить степень достижения учебных целей по учебной дисциплине и проводится в форме зачета. Принимается зачет

преподавателями, читающими лекции по данной учебной дисциплине в соответствии с перечнем основных вопросов, выносимых для контроля знаний обучающихся.

7.1. Вопросы к зачету

1. Понятие кольца.
2. Математическое моделирование аффинного шифра.
3. Делимость в кольце целых чисел.
4. Наибольший общий делитель и наименьшее общее кратное.
5. Алгоритм Евклида.
6. Функция Эйлера.
7. Бинарный и расширенный алгоритмы Евклида.
8. Простые числа и их свойства. Распределение простых чисел.
9. Понятие простого конечного поля.
10. Отношение сравнимости.
11. Сравнения первой степени и их решение.
12. Китайская теорема об остатках.
13. Сравнения второй степени.
14. Символы Лежандра и Якоби.
15. Извлечение квадратного корня по модулю простого числа.
16. Алгоритм Шенкса. Модульное возведение в степень.
17. Малая теорема Ферма.
18. Обобщение Эйлера для малой теоремы Ферма.
19. Задача RSA.
20. Протокол Диффи-Хеллмана.
21. Криптосистема Эль-Гамаля.
22. Простейшая арифметика в кольце многочленов.
23. Алгоритм Евклида для многочленов. Теорема Лагранжа.
24. Поля Галуа. Характеристика поля.
25. Поле разложения многочлена.
26. Решение систем линейных уравнений над конечным полем.
27. Оптимальные базисы.
28. Неприводимые многочлены.
29. Определение непрерывной дроби.
30. Подходящие дроби.
31. Квадратичные иррациональности.
32. Непрерывные дроби в решении задач.
33. Простейшие Диофантовы уравнения.
34. Уравнение Пелля.
35. Представление числа в виде суммы квадратов.
36. Разложение функций в непрерывные дроби.
37. Умножение методом Карацубы-Оффмана.
38. Умножение в классах вычетов.
39. Дискретное преобразование Фурье.
40. Умножение с помощью быстрого преобразования Фурье.
41. Алгоритм Шенхаге-Штрассена.
42. Модульное умножение.
43. Метод Монтгомери.
44. Модульное возведение в степень.
45. Потенцирование методом «разделяй и властвуй».
46. Параллельное потенцирование и умножение.
47. Целочисленное деление с остатком.
48. Приведение по модулю.
49. Схема Горнера.

50. Решето Эратосфена.
51. Вероятностные алгоритмы проверки чисел по на простоту.
52. Тест Ферма.
53. Тест Соловэя-Штрассена.
54. Тест Миллера-Рабина.
55. Генерация простого числа.
56. Детерминированные алгоритмы проверки чисел на простоту.
57. Тестирование и поиск неприводимых многочленов.
58. Ассимптотически быстрые и вероятностные тесты многочленов на неприводимость.
59. Пробное деление.
60. Ро-методы Полларда.
61. Метод квадратов.
62. Метод непрерывных дробей.
63. Метод квадратичного решета.
64. Взаимосвязь компонентов RSA.
65. Задача дискретного логарифмирования.
66. Ро-метод Полларда.
67. Методы Гельфонда и Сильвера-Полига-Хеллмана.
68. Метод встречи посередине.
69. Метод базы разложения.
70. Процесс ортогонализации Грама-Шмидта.
71. Алгоритм Ленстры-Ленстры-Ловаша и его применение.
72. Задача об укладке ранца.
73. Ранцевые алгоритмы шифрования.
74. Алгебраические кривые и эллиптические кривые.
75. Однородное уравнение Вейерштрасса.
76. Группа точек эллиптической кривой.
77. Аномальные и суперсингулярные кривые.
78. Групповой закон.
79. Порядок эллиптической кривой над конечным полем.
80. Теорема Хассе.
81. Скалярное умножение.

7.2. Оценивание результатов зачета.

Зачет проводится по окончании занятий по дисциплине до начала экзаменационной сессии в период недели контроля самостоятельной работы.

Билет для проведения промежуточной аттестации в форме зачета включают вопросы и задачи для проверки сформированности знаний, умений и навыков.

Оценка «зачтено» проставляется студенту, выполнившему и защитившему в полном объеме лабораторные работы в течение семестра, имеются твердые и полные знания программного материала, правильные действия по применению знаний на практике, четкое изложение материала

Оценка «не зачтено» проставляется студенту, не выполнившему и (или) не защитившему в полном объеме лабораторные работы в течение семестра, либо наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять знания на практике, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

8. Учебно-методическое и информационное обеспечение дисциплины

Электронный каталог и электронные информационные ресурсы, предоставляемые научной библиотекой ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова» доступны по ссылке http://library.chuvsu.ru/

8.1. Рекомендуемая основная литература

Ежегодное обновление и условия доступа перечня представлены в Приложениях к рабочей программе.

№ п/п	Наименование
1.	Романьков В.А. Алгебраическая криптография [Электронный ресурс] : монография / В.А. Романьков. — Электрон. текстовые данные. — Омск: Омский государственный университет им. Ф.М. Достоевского, 2013. — 136 с. — 978-5-7779-1600-6. — Режим доступа: http://www.iprbookshop.ru/24868.html
2.	Аграновский А.В. Практическая криптография. Алгоритмы и их программирование [Электронный ресурс] / А.В. Аграновский, Р.А. Хади. — Электрон. текстовые данные. — М. : СОЛОН-ПРЕСС, 2009. — 256 с. — 5-98003-002-6. — Режим доступа: http://www.iprbookshop.ru/8641.html
3.	Петров А.А. Компьютерная безопасность. Криптографические методы защиты [Электронный ресурс] / А.А. Петров. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 446 с. — 978-5-4488-0091-7. — Режим доступа: http://www.iprbookshop.ru/63800.html

8.2. Рекомендуемая дополнительная литература

Ежегодное обновление и условия доступа перечня представлены в Приложениях к рабочей программе.

№ п/п	Наименование
1.	Басалова Г.В. Основы криптографии [Электронный ресурс] / Г.В. Басалова. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 282 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/52158.html
2.	Жидко Е.А. Логико-вероятностно-информационный подход к моделированию информационной безопасности объектов защиты [Электронный ресурс] : монография / Е.А. Жидко. — Электрон. текстовые данные. — Воронеж: Воронежский государственный архитектурно-строительный университет, ЭБС АСВ, 2016. — 121 с. — 978-5-89040-614-9. — Режим доступа: http://www.iprbookshop.ru/72917.html
3.	Соколов В.П. Кодирование в системах защиты информации [Электронный ресурс] : учебное пособие / В.П. Соколов, Н.П. Тарасова. — Электрон. текстовые данные. — М. : Московский технический университет связи и информатики, 2016. — 94 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/61485.html

8.4. Программное обеспечение, профессиональные базы данных, информационно-справочные системы.

Нормативные правовые и методические документы в области защиты информации доступны по ссылке https://fstec.ru/component/tags/tag/informatsionnoe-soobshchenie

Программное обеспечение, профессиональные базы данных, информационно-справочные системы, предоставляемые управлением информатизации ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова» доступны по ссылке http://ui.chuvsu.ru//

8.3.1 Программное обеспечение

№ п/п	Наименование	Условия доступа/скачивания
1.	MS Windows/ Arch linux	лицензия университета/ свободное лицензионное соглашение (https://www.archlinux.org/download/)
2.	MS Office/ LibreOffice	лицензия университета/ свободное лицензионное соглашение (https://ru.libreoffice.org/)
3.	Visual Studio Community	http://www.visualstudio.com/ru/vs/community

8.3.2 Базы данных, информационно-справочные системы

№ п/п	Наименование программного обеспечения	Условия доступа/скачивания
1.	Гарант	из внутренней сети университета (договор)*
2.	Консультант +	

8.4. Рекомендуемые интернет-ресурсы и открытые онлайн курсы.

№ п/п	Наименование	Условия доступа
1.	Российская Государственная Библиотека	http://www.rsl.ru
2.	Государственная публичная научно-техническая библиотека России	http://www.gpntb.ru

3.	Фундаментальная библиотека Нижегородского государственного университета	http://www.unn.ru/library
4.	Научная библиотека Казанского государственного университета	http://lsl.ksu.ru
5.	Научная электронная библиотека	http://elibrary.ru
6.	Полнотекстовая библиотека учебных и учебно-методических материалов	http://window.edu.ru
7.	Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru
8.	ISO 27000 Международные стандарты управления информационной безопасностью.	URL: http://iso27000.ru
9.	Информационная безопасность. Практика информационной безопасности.	URL: dorlov.blogspot.com
10.	SecurityLab. Информационный портал по безопасности.	URL: www.securitylab.ru

9. Материально-техническое обеспечение дисциплины

Учебные аудитории для лекционных занятий по дисциплине оснащены автоматизированным рабочим местом (АРМ) преподавателя, обеспечивающим тематические иллюстрации и демонстрации, соответствующие программе дисциплины в составе:

– ПЭВМ с доступом в интернет (операционная система, офисные программы, антивирусные программы);

– мультимедийный проектор с дистанционным управлением;

Учебные аудитории для практических, лабораторных и самостоятельных занятий по дисциплине оснащены АРМ преподавателя и пользовательскими АРМ по числу обучающихся, объединенных локальной сетью («компьютерный» класс), с возможностью подключения к сети Интернет и доступом к электронной информационно-образовательной среде ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова».

10. Средства адаптации преподавания дисциплины к потребностям лиц с ограниченными возможностями

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться одни из следующих вариантов восприятия информации с учетом их индивидуальных психофизических особенностей, в том числе с применением электронного обучения и дистанционных технологий:

– для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации.

– для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации.

– для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

11. Методические рекомендации по освоению дисциплины

В ходе лекционных занятий студенту рекомендуется вести конспектирование учебного материала. Следует обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации, положительный опыт в ораторском искусстве. При составлении конспекта

желательно оставлять в рабочих конспектах поля, на которых в дальнейшем можно делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. В ходе лекционных занятий рекомендуется задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

В ходе подготовки к практическим занятиям и лабораторным работам рекомендуется изучить основную литературу, ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях. основой для выполнения лабораторной работы являются разработанные кафедрой методические указания. Рекомендуется дорабатывать свой конспект лекций, делая в нем соответствующие записи из литературы, рекомендованной преподавателем и предусмотренной рабочей программой дисциплины. Желательно подготовить тезисы для выступлений по всем учебным вопросам, выносимым на практическое занятие. Готовясь к докладу или реферативному сообщению, рекомендуется обращаться за методической помощью к преподавателю, составить план-конспект своего выступления, продумать примеры с целью обеспечения тесной связи изучаемой теории с практикой. В процессе подготовки студент может дополнить список использованной литературы современными источниками, не представленными в списке рекомендованной литературы, и в дальнейшем использовать собственные подготовленные учебные материалы при написании выпускной квалификационной работы.

Формы организации студентов на лабораторных работах и практических занятиях: фронтальная. При фронтальной форме организации занятий все студенты выполняют одновременно одну и ту же работу.

Если в результате выполнения лабораторной работы запланирована подготовка письменного отчета, то отчет о выполненной работе необходимо оформлять в соответствии с требованиями методических указаний. Качество выполнения лабораторных работ является важной составляющей оценки текущей успеваемости обучающегося.