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
«КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ»

Специальность 10.05.03 – Информационная безопасность автоматизированных систем

Квалификация (степень) выпускника - Специалист по защите информации

Профиль (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 Минобрнауки 01.12.2016 г. №1509

СОСТАВИТЕЛЬ (СОСТАВИТЕЛИ):
Доцент, к.ф.-м.н. Д.В. Ильин
Старший преподаватель С.Ю. Манюков

ОБСУЖДЕНО:
на заседании кафедры математического и аппаратного обеспечения информацион-ных систем 30.08.2017 г., протокол № 1

заведующий кафедрой Д.В. Ильин

СОГЛАСОВАНО:
Методическая комиссия факультета информатики и вычислительной техники
«30» августа 2017г., 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 освоения дисциплины

Цель дисциплины: изложение основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике.

Задачи дисциплины:

Обеспечить освоение основ:

- системного подхода к организации защиты информации, передаваемой иобрабатываемойтехническимисредствамина основеприменениякриптографическихметодов;
- принципов разработки шифров;
- математических методов, используемых в криптографии.

2. Место дисциплины в структуре ООП ВО

Дисциплина «Криптографические методы защиты информации» (КМЗИ) относится к базовой части образовательной программы. КМЗИ формирует фундаментальные и прикладные знания о защите информации с помощью криптографических методов.

Изучение дисциплины «Криптографические методы защиты информации» основывается на базе знаний, умений и владений, полученных обучающимися в ходе освоения дисциплин: «Алгебра», «Математическая логика и теория алгоритмов», «Языки программирования», «Информатика», «Дискретная математика».

КМЗИ является теоретическим и практическим основанием для: прохождения практик, государственной итоговой аттестации.

3. Компетенции обучающихся, формируемые в результате освоения дисциплины, ожидаемые результаты образования

В процессе освоения данной дисциплины обучающиеся формируют следующие компетенции и демонстрирует соответствующие им результаты обучения:

ОПК-3 – способность применять языки, системы и инструментальные средства программирования в профессиональной деятельности;

ПК-10 – способность применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности;

ПК-25 – способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций.

Знать

- основные задачи и понятия криптографии (З1);
- требования к шифрам и основные характеристики шифров (З2);
- модели шифров и математические методы их исследования (З3);
- принципы построения криптографических алгоритмов;
- криптографические стандарты (З4);
- способы использования криптографических стандартов в информационных системах (З5);
- о системах криптографической защиты информации (СКЗИ) (З6);

Уметь

- применять криптографические алгоритмы на практике (У1);

применять отечественные и зарубежные стандарты в области криптографических методов компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем (У2);

- осуществлять программную реализацию криптографических алгоритмов (У3);
- пользоваться научно-технической литературой в области криптографии (У4).

Владеть

- криптографической терминологией (Н1);
- навыками программной реализации криптографических алгоритмов (Н2);
- навыками использования типовых криптографических алгоритмов (Н3);
- навыками использования ПЭВМ в анализе шифров (Н4);
- навыками математического моделирования в криптографии (Н5);
- средствами обеспечения информационной безопасности (Н6);
- навыками определения видов и форм информации, подверженных угрозам, и возможных методов и путей устранения этих угроз (Н7).

4. Структура и содержание дисциплины

4.1. Структура дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела	Формируемые компетенции (ОК, ОПК, ПК)
1.	Раздел 1. Основы криптографии.	Введение в криптографию. История криптографии. Исторические шифры. Математическая модель шифра. Теория секретности Шеннона.	ОПК-3, ПК-10 ПК-25
2.	Раздел 2. Симметричные криптосистемы.	Блочные шифры. Псевдослучайные последовательности и поточные шифры. Теория имитостойкости Симмонса и криптографические хэш-функции.	ОПК-3, ПК-10 ПК-25
3.	Раздел 3. Асимметричные криптосистемы и протоколы.	Асимметричные (с открытым ключом) шифры. Схемы цифровой подписи. Эллиптические кривые над конечным полем. Шифры и ЭЦП на их основе. Введение в криптографические протоколы.	ОПК-3, ПК-10 ПК-25

4.2. Объем дисциплины и виды учебной работы для очной формы обучения

№ п/п	Аудиторные занятия	Контактная работа, в т.ч. в электронной информационно-образовательной среде			Самостоятельная работа	Контроль самост. работы	Контроль	Всего часов	Из них в интерактивной форме
		Лекции	Практические занятия	Лабораторные занятия					
1.	Раздел 1. Основы криптографии.								
2.	Тема 1. Введение в криптографию.	2			2			4	2
3.	Тема 2. История криптографии. Исторические шифры.	4			2			6	4
4.	Тема 3. Математическая модель шифра. Теория секретности Шеннона.	4		4	4			12	4
5.	Раздел 2. Симметричные криптосистемы.								
6.	Тема 4. Блочные шифры.	4		4	4			12	4
7.	Тема 5. Псевдослучайные последовательности и поточные шифры.	4		4	4			12	4
8.	Тема 6. Теория имитостойкости Симмонса и криптографические хэш-функции.	4		4	4			12	4
9.	Раздел 3. Асимметричные криптосистемы и протоколы.								

10.	Тема 7. Асимметричные(с открытым ключом) шифры.	4		6	4			14	4
11.	Тема 8. Схемы цифровой подписи.	2		4	4			10	2
12.	Тема 9. Эллиптические кривые над конечным полем. Шифры и ЭЦП на их основе.	2		4	4			10	2
13.	Тема 10. Введение в криптографические протоколы.	2		2	8			12	2
	Зачет				2			2	
	Курсовой проект					2		2	
	Экзамен						36	36	
	Итого, час.	32		32	42	2		144	32
	Итого, з.е.							4	

4.3 Темы занятий и краткое содержание

Раздел 1. Основы криптографии

Тема 1. Введение в криптографию.

Лекция 1. Введение в криптографию.

Основные понятия и определения. Виды криптосистем. Задачи, решаемые методами криптографии. Виды информации, подлежащие закрытию, их модели и свойства. Частотные характеристики открытых сообщений. Критерии на открытый текст. Особенности нетекстовых сообщений.

Тема 2. История криптографии. Исторические шифры.

Лекция 2. История криптографии. Исторические шифры.

Основныеэтапыстановлениякриптографиикакнауки.Классификацияшифров.Шифрызаме ны, перестановки, гаммирования. Композиции шифров. Примеры исторических ручных и машинных шифров. Шифр Цезаря. Шифр простой замены. Шифр Плейфера. Полибианский квадрат. Шифр Хилла. Шифр Виженера. Шифр«Решетка».Шифр Вернама. Enigma. Шифр Хейглина. Способы их скрытия. Блочные и поточные шифры.

Тема 3. Математическая модель шифра. Теория секретности Шеннона.

Лекция 3. Математическая модель шифра. Теория секретности Шеннона.

Алгебраическая модель, вероятностная модель. Атаки и угрозы шифрам. Вычислительная и теоретическая стойкость. Теоретико-информационный подход к оценке стойкости шифров. Криптографическая стойкость шифров. Совершенные шифры. Энтропийные характеристики шифров. Идеальные шифры. Избыточность языка. Оценка числа ложных ключей и расстояние единственности. Безусловно стойкие и вычислительно стойкие шифры. Вопросы практической стойкости.

Лабораторная работа 1 (4 часа). Построение математических моделей шифров. Оценка их криптографической стойкости.

Раздел 2. Симметричные криптосистемы.

Тема 4. Блочные шифры.

Лекция 4. Блочные шифры.

Понятие о блочном шифре. Замены и перестановки. S-Pсеть. Лавинный эффект. Сеть Файстеля. Шифр ГОСТ28147-89. Шифры SQUARE, AES. Подходы к криптоанализу блочных шифров. Дифференциальный криптоанализ. Линейный криптоанализ. Режимы шифрования. Многократное шифрование и атака «встреча посередине». Композиция блочных шифров.

Лабораторная работа 2 (4 часа). Построение и реализация блочных шифров.

Тема 5. Псевдослучайные последовательности и поточные шифры.

Лекция 5. Псевдослучайные последовательности и поточные шифры.

Характеристики генераторов псевдослучайных последовательностей (ПСП, ПСГ). Требования к криптографическим ПСП. Примеры ПСГ и криптографических ПСГ.

Лекция 6. Псевдослучайные последовательности и поточные шифры.

Общая схема поточного шифра. Синхронные и самосинхронизирующиеся шифры. Регистры сдвига с обратной линейной связью (РСЛОС). ПСГ на основе РСЛОС. Шифр Trivium. Нелинейные регистры сдвига. Другие поточные шифры– RC4.

Лабораторная работа 3 (4 часа). Построение и реализация поточных шифров

Тема 6. Теория имитостойкости Симмонса и криптографические хэш-функции.

Лекция 7. Теория имитостойкости Симмонса и криптографические хэш-функции.

Имитация и подмена сообщения. Характеристики имитостойкости. Методы обеспечения имитостойкости шифров. Совершенная имитостойкость. Связь между имитостойкостью по Симмонсу и секретностью по Шеннону. Понятие кода аутентификации и его свойства имитостойкости и секретности

Лекция 8. Теория имитостойкости Симмонса и криптографические хэш-функции.

Назначение и конструкция кодов аутентификации защитных контрольных сумм. Требования к хэш-функциям. Криптографическая стойкость хэш-функций. Коллизии. Применение хэш-функций.

Лекция 9. Теория имитостойкости Симмонса и криптографические хэш-функции.

Подходы к проектированию хэш-функций. Алгоритмы выработки хэш-функций. Хэш-функции на основе блочного шифра. Стандарты на хэш-функции: ГОСТР 34.11-94, SHA-1. Схема Меркла-Дамгарда и ГОСТР 34.11-2012. Концепция «губка» и SHA-3. Коды аутентификации и способы их построения. HMAC.

Лабораторная работа 4 (4 часа). Построение и реализация хэш-функций.

Раздел 3. Асимметричные криптосистемы и протоколы

Тема 7. Асимметричные (с открытым ключом) шифры

Лекция 10.Асимметричные(с открытым ключом) шифры.

Понятие односторонней функции и односторонней функции с "лазейкой". Проблемы факторизации целых чисел и логарифмирования в конечных полях. Криптосистема Диффи-Хэллмана. Криптосистемы RSA, Эль-Гамаля, Рабина, Гольдвассер-Микали, Блюма-Гольдвассер

Лекция 11. Асимметричные (с открытым ключом) шифры.

Рюкзачные шифры. Криптосистемы с открытым ключом, основанные на линейных кодах. Преимущества и недостатки асимметричных систем шифрования. Генерация ключевой информации для асимметричных криптосистем. Вероятностные тесты на простоту. Доказуемо простые числа. Нахождение порождающего элемента и элемента заданного порядка.

Лабораторная работа 5 (6 часа). Построение и реализация ассиметричных шифров (с открытым ключом).

Тема 8. Схемы цифровой подписи

Лекция 12. Схемы цифровой подписи.

Понятие электронной цифровой подписи и требования к ней. Атаки и угрозы схемам ЭЦП.

Лекция 13. Схемы цифровой подписи.

Алгоритмы ЭЦП: RSA, Эль-Гамаля, Фиата-Шамира, Онга-Шнорра-Шамира, Шнорра. Неотрицаемая подпись Шаума-ван-Антверпена. Стандарты ЭЦП: DSS, ГОСТР 34.10-94.

Лабораторная работа 6 (4 часа). Построение и реализация алгоритмов ЭЦП.

Тема 9. Эллиптические кривые над конечным полем. Шифры и ЭЦП на их основе

Лекция 14. Эллиптические кривые над конечным полем. Шифры и ЭЦП на их основе.

Эллиптическая кривая над конечным полем. Операции на эллиптической кривой. Сумма точек. Кратная точка. Проблема дискретного логарифмирования на эллиптической кривой. Переход от шифра (ЭЦП) в Z_pк шифру (ЭЦП) на эллиптической

кривой. Шифр Эль-Гамаля на эллиптической кривой. Стандарты ЭЦП на эллиптической кривой: ГОСТР 34.10-2001, ГОСТР 34.10-2012, ECDSA

Лабораторная работа 7 (4 часа). Построение и реализация шифров на основе эллиптической кривой.

Тема 10. Введение в криптографические протоколы.

Лекция 15. Введение в криптографические протоколы.

Понятие криптографического протокола. Основные примеры. Связь стойкости протокола со стойкостью базовой криптографической системы. Классификация криптографических протоколов. Парольные схемы и протоколы" рукопожатия". Взаимосвязь между протоколами аутентификации цифровой подписи.

Лекция 16. Введение в криптографические протоколы.

Протоколы сертификации ключей. Протоколы предварительного распределения ключей. Протоколы выработки сеансовых ключей. Открытое распределение ключей Диффи-Хеллмана и его модификации. Вопросы организации сетей засекреченной связи. Доказательства с нулевым разглашением. Разделение секрета. Протоколы подбрасывания монеты. Построение протоколов с нулевым разглашением на основе NP-сложных задач.

Лабораторная работа 8 (2 часа). Построение криптографических протоколов.

5. Образовательные технологии

Составными элементами образовательных технологий являются:

лекции – для изложения нового материала также используется интерактивная форма проведения занятия.

лабораторные занятия – проводятся в компьютерных классах на современных персональных компьютерах с использованием специальных пакетов прикладных программ;

применение мультимедийных средств (электронные доски, проекторы) – для повышения качества восприятия изучаемого материала.

№ темы	Вид занятия (лекция, практическое занятие, лабораторное занятие)	Используемые интерактивные технологии	Всего часов
1-8	Лабораторные занятия	Компьютерная симуляция, метод проектов	32

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

Формы и виды контроля знаний обучающихся, предусмотренные по данной дисциплине:

- текущий контроль (защита лабораторных работ, выполнение аудиторных проверочных работ);
- промежуточная аттестация (зачёт, экзамен, защита курсового проекта).

Контрольные мероприятия и соответствующие им максимальные баллы по экзамену:

№	Контрольные мероприятия	Максимальные баллы
1	Защита лабораторной работы №1	5
2	Защита лабораторной работы№2	5
3	Защита лабораторной работы№3	5
4	Защита лабораторной работы №4	5
5	Защита лабораторной работы №5	5
6	Защита лабораторной работы №6	5
7	Защита лабораторной работы №7	5
8	Защита лабораторной работы №8	5
9	Зачёт	20
10	Экзамен	40

	Сумма	100

Критерии экзаменационной оценки:

Оценка формируется путем перевода накопленной в течение обучения суммы баллов обучающегося по следующей шкале:

«отлично» – 76 баллов и выше.

«хорошо» – от 56 до 75 баллов;

«удовлетворительно» – от 41 до 55 баллов;

«неудовлетворительно» - до 40 баллов.

Оценка «отлично» выставляется, если студент набрал не менее 76 баллов и показал глубокое и полное знание материала учебной дисциплины, усвоение основной и дополнительной литературы, рекомендованной рабочей программой учебной дисциплины.

Оценки «хорошо» выставляется студенту, набравшему не менее 56 баллов и показавшему полное знание основного материала учебной дисциплины, знание основной литературы и знакомство с дополнительной литературой, рекомендованной рабочей программой.

Оценки «удовлетворительно» выставляется, если студент, набрал не менее 41 балла и показал при ответе на экзамене знание основных положений учебной дисциплины, допустил отдельные погрешности и сумел устранить их с помощью преподавателя, знаком с основной литературой по предмету.

Оценка «неудовлетворительно» выставляется, если студент набрал менее 41 балла и при ответе выявились существенные пробелы в знании основных положений учебной дисциплины, неумение студента даже с помощью преподавателя сформулировать правильные ответы на вопросы.

6.1. Примерный перечень вопросов к зачету

1. Основные понятия и определения криптографии.
2. Виды криптосистем. Задачи, решаемые методами криптографии.
3. Виды информации, подлежащие закрытию, их модели свойства. Частотные характеристики открытых сообщений. Критерии на открытый текст. Особенности не текстовых сообщений.
4. История криптографии. Основные этапы становления науки криптографии.
5. Классификация шифров замены. Шифр Цезаря. Шифр простой замены. Шифр Плейфера. Полибианский квадрат. Шифр Хилла. Шифр Виженера. Частотный анализ. Тест Казиски.
6. Классификация шифров перестановки. Примеры шифров перестановки и их криптоанализ.
7. Шифры гаммирования. Шифр Вернама. Подходы к его криптоанализу.
8. Композиции шифров. Enigma. Шифр Хейглина.
9. Математическая модель шифра.
10. Атаки и угрозы шифрам.
11. Блочные шифры и их ключевая система. Замены и перестановки. S-P-сеть.
12. Сеть Файстеля. Шифр ГОСТ 28147-89.
13. Конечные кольца и поля многочленов.
14. Шифр SQUARE.
15. Шифр AES
16. Режимы шифрования.
17. Многократное шифрование. Композиция блочных шифров.
18. Совершенные шифры. Пример совершенного шифра.
19. Энтропийные характеристики шифров. Идеальные шифры.
20. Избыточность языка.

21. Оценка числа ложных ключей и расстояние единственности.
22. Безусловно стойкие и вычислительно стойкие шифры.
23. Псевдослучайные последовательности (ПСП). Характеристики генераторов ПСП (ПСГ). Требования к криптографическим ПСП. Примеры ПСГ и криптографических ПСГ.
24. Поточные шифры. Общая схема поточного шифра. Синхронные и самосинхронизирующиеся шифры.
25. Регистры сдвига с обратной линейной связью(РСЛОС).
26. ПСГ на основе РСЛОС.
27. Шифр Trivium.
28. Нелинейные регистры сдвига.
29. Шифр RC4.
30. ТеорияимитостойкостиСиммонса.Имитацияиподменасообщения.Характеристиимитостойкости.Совершеннаяимитостойкость.
31. Коды аутентификации сообщений.
32. Защитные контрольные суммы.
33. Криптографические хэш-функции и требования к ним.
34. Подходы к проектированию хэш-функций.
35. Хэш-функции на основе блочного шифра.
36. Схема Меркла-ДамгардаиГОСТР34.11-2012.
37. Схема«губка»иSHA-3.
38. Коды аутентификации сообщений.
39. Понятие односторонней функции односторонней функции с"лазейкой". Проблемы факторизации целых чисел и логарифмирования в конечных полях.
40. Криптосистема Диффи-Хэллмана. Пример.
41. Криптосистема RSA. Пример.
42. Криптосистема Эль-Гамаля. Пример.
43. Криптосистема Рабина. Пример.
44. Криптосистема Гольдвассер-Микали. Пример.
45. Криптосистема Блюма-Гольдвассер. Пример.
46. Рюкзачные шифры. Криптосистема Меркла-Хэллмана.
47. Понятие электронной цифровой подписи и требования к ней. Атаки и угрозы схемам ЭЦП.
48. Подпись RSA, Эль-Гамаля.
49. Подпись Фиата-Шамира.
50. Подпись Онга-Шнорра-Шамира.
51. Неотрицаемая подпись Шаума-ван-Антверпена.
52. Стандарты ЭЦП: DSS, ГОСТР 34.10-94.
53. Эллиптическая кривая над конечным полем. Операции на эллиптической кривой. Сумма точек. Кратная точка.
54. Проблема дискретного логарифмирования на эллиптической кривой. Переход от шифра(ЭЦП) в Z_p к шифру (ЭЦП) на эллиптической кривой.
55. Шифр Эль-Гамаля на эллиптической кривой.
56. Стандарты ЭЦП на эллиптической кривой: ГОСТР 34.10-2001(2012),ECDSA

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.

Оценивание результатов зачета осуществляется в соответствии с полнотой и качеством выполнения задания на работу, качеством защиты работы (ответы на вопросы, и др.). Оценка работы отражает уровень сформированности соответствующих

компетенций.

– «отлично» - работа выполнена в соответствии с утвержденным планом и заданием, полностью раскрыто содержание каждого вопроса; студентом сформулированы собственные аргументированные выводы по теме работы; оформление работы соответствует предъявляемым требованиям; при защите работы обучающийся демонстрирует свободное владение материалом и верно отвечает на поставленные вопросы;

– «хорошо» - работа выполнена в соответствии с утвержденным планом и заданием; полностью раскрыто содержание каждого вопроса; имеются незначительные замечания к оформлению работы; при защите работы обучающийся демонстрирует владение материалом, но отвечает на ряд поставленных вопросов не в достаточно полном объеме;

– «удовлетворительно» - работа выполнена в соответствии с утвержденным планом и заданием, но не полностью раскрыто содержание каждого вопроса; обучающимся не сделаны собственные выводы по теме работы; допущены существенные недостатки в оформлении работы; при защите работы обучающийся демонстрирует владение материалом, но отвечает не на все поставленные вопросы, либо не в достаточно полном объеме;

– «неудовлетворительно» - если работа не выполнена в соответствии с утвержденным планом и заданием, не раскрыто содержание каждого вопроса; обучающимся не сделаны выводы по теме работы, имеются существенные недостатки в оформлении работы; при защите работы обучающийся не демонстрирует владение материалом, не отвечает на поставленные вопросы.

Оценка «зачтено» проставляется студенту, выполнившему и защитившему в полном объеме практические задания и лабораторные работы в течение семестра, чей уровень знаний, умений и навыков соответствует уровню оценок «отлично», «хорошо» или «удовлетворительно». Оценка «не зачтено» проставляется студенту, не выполнившему и (или) не защитившему в полном объеме практические задания и лабораторные работы в течение семестра, либо чей уровень знаний, умений и навыков соответствует уровню оценки «неудовлетворительно».

6.2. Примерный перечень вопросов к экзамену

1. Основные понятия и определения криптографии.
2. Виды криптосистем. Задачи, решаемые методами криптографии.
3. Виды информации, подлежащие закрытию, их модели свойства. Частотные характеристики открытых сообщений. Критерии на открытый текст. Особенности не текстовых сообщений.
4. История криптографии. Основные этапы становления науки криптографии.
5. Классификация шифров замены. Шифр Цезаря. Шифр простой замены. Шифр Плейфера. Полибианский квадрат. Шифр Хилла. Шифр Виженера. Частотный анализ. Тест Казиски.
6. Классификация шифров перестановки. Примеры шифров перестановки и их криптоанализ.
7. Шифры гаммирования. Шифр Вернама. Подходы к его криптоанализу.
8. Композиции шифров. Enigma. Шифр Хейглина.
9. Математическая модель шифра.
10. Атаки и угрозы шифрам.
11. Блочные шифры и их ключевая система. Замены и перестановки. S-P-сеть.
12. Сеть Файстеля. Шифр ГОСТ 28147-89.
13. Конечные кольца и поля многочленов.
14. Шифр SQUARE.
15. Шифр AES

16. Режимы шифрования.
17. Многократное шифрование. Композиция блочных шифров.
18. Совершенные шифры. Пример совершенного шифра.
19. Энтропийные характеристики шифров. Идеальные шифры.
20. Избыточность языка.
21. Оценка числа ложных ключей и расстояние единственности.
22. Безусловно стойкие и вычислительно стойкие шифры.
23. Псевдослучайные последовательности (ПСП). Характеристики генераторов ПСП (ПСГ). Требования к криптографическим ПСП. Примеры ПСГ и криптографических ПСГ.
24. Поточные шифры. Общая схема поточного шифра. Синхронные и самосинхронизирующиеся шифры.
25. Регистры сдвига с обратной линейной связью(РСЛОС).
26. ПСГ на основе РСЛОС.
27. Шифр Trivium.
28. Нелинейные регистры сдвига.
29. Шифр RC4.
30. ТеорияимитостойкостиСиммонса.Имитацияиподменасообщения.Характеристикиимитостойкости.Совершеннаяимитостойкость.
31. Коды аутентификации сообщений.
32. Защитные контрольные суммы.
33. Криптографические хэш-функции и требования к ним.
34. Подходы к проектированию хэш-функций.
35. Хэш-функции на основе блочного шифра.
36. Схема Меркла-ДамгардаиГОСТР34.11-2012.
37. Схема«губка»иSHA-3.
38. Коды аутентификации сообщений.
39. Понятие односторонней функции односторонней функции с"лазейкой". Проблемы факторизации целых чисел и логарифмирования в конечных полях.
40. Криптосистема Диффи-Хэллмана. Пример.
41. Криптосистема RSA. Пример.
42. Криптосистема Эль-Гамаля. Пример.
43. Криптосистема Рабина. Пример.
44. Криптосистема Гольдвассер-Микали. Пример.
45. Криптосистема Блюма-Гольдвассер. Пример.
46. Рюкзачные шифры. Криптосистема Меркла-Хэллмана.
47. Понятие электронной цифровой подписи и требования к ней. Атаки и угрозы схемам ЭЦП.
48. Подпись RSA, Эль-Гамаля.
49. Подпись Фиата-Шамира.
50. Подпись Онга-Шнорра-Шамира.
51. Неотрицаемая подпись Шаума-ван-Антверпена.
52. Стандарты ЭЦП: DSS, ГОСТР 34.10-94.
53. Эллиптическая кривая над конечным полем. Операции на эллиптической кривой. Сумма точек. Кратная точка.
54. Проблема дискретного логарифмирования на эллиптической кривой. Переход от шифра(ЭЦП) в Z_p к шифру (ЭЦП) на эллиптической кривой.
55. Шифр Эль-Гамаля на эллиптической кривой.
56. Стандарты ЭЦП на эллиптической кривой: ГОСТР 34.10-2001(2012),ECDSA

Экзаменационный билет для проведения промежуточной аттестации включают вопросы и задачи для проверки сформированности знаний, умений и навыков.

Общими критериями, определяющими оценку знаний, умений и навыков на экзамене, являются:

для оценки «отлично» - наличие глубоких и исчерпывающих знаний в объёме пройденного программного материала правильные и уверенные действия по применению полученных знаний на практике, грамотное и логически стройное изложение материала при ответе, знание дополнительно рекомендованной литературы;

для оценки «хорошо» - наличие твердых и достаточно полных знаний программного материала, незначительные ошибки при освещении заданных вопросов, правильны действия по применению знаний на практике, четкое изложение материала;

для оценки «удовлетворительно» - наличие твердых знаний пройденного материала, изложение ответов с ошибками, уверенно исправляемыми после дополнительных вопросов, необходимость наводящих вопросов, правильные действия по применению знаний на практике;

для оценки «неудовлетворительно» - наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять знания на практике, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

6.3. Примерная тематика курсовых проектов

Тематика курсовых проектов ориентирована на самостоятельное изучение студентами и программную реализацию современных блочных и поточных шифров, прикладных криптографических протоколов и иных криптосистем, имеющих теоретическую, историческую или практическую ценность, являющихся победителями ведущих мировых криптографических конкурсов либо использующихся в современных широко известных СКЗИ, являющихся частью мировых и линациональных стандартов. Помимо тем из ниже приведенного списка пожеланию студента и по согласованию с преподавателем может быть избрана иная тема, соответствующая выше приведенном у критерию.

1. Блочный шифр Serpent.
2. Блочный шифр Twofish.
3. Блочный шифр RC6.
4. Блочный шифр MARS.
5. Первый блочный шифр Lucifer и его криптоанализ.
6. Поточный шифр HC-128.
7. Поточный шифр Rabbit.
8. Поточный шифр Salsa 20/12.
9. Поточный шифр SOSEMANUK.
10. Поточный шифр Grain.
11. Поточный шифр Mickey.
12. Блочный шифр Camellia и область его применения.
13. Шифр Blowfish и область его применения.
14. Шифр CASTи область его применения

Оценивание курсового проекта

Курсовой проект выполняется в процессе изучения дисциплины. Общее руководство и контроль за ходом выполнения курсового проекта осуществляет преподаватель соответствующей дисциплины. Курсовой проект выполняется в соответствии с методическими указаниями для обучающихся.

Оценивание курсового проекта осуществляется в соответствии с полнотой и качеством выполнения задания на курсовой проект, качеством защиты проекта (ответы на вопросы, презентация и др.). Оценка курсового проекта отражает уровень сформированности соответствующих (п. 7.2) компетенций:

– «отлично» - проект выполнен в соответствии с утвержденным планом и заданием, полностью раскрыто содержание каждого вопроса; студентом сформулированы собственные аргументированные выводы по теме работы; оформление работы соответствует предъявляемым требованиям; при защите работы обучающийся демонстрирует свободное владение материалом и верно отвечает на поставленные вопросы;

– «хорошо» - проект выполнен в соответствии с утвержденным планом и заданием; полностью раскрыто содержание каждого вопроса; имеются незначительные замечания к оформлению работы; при защите работы обучающийся демонстрирует владение материалом, но отвечает на ряд поставленных вопросов не в достаточно полном объеме;

– «удовлетворительно» - проект выполнен в соответствии с утвержденным планом и заданием, но не полностью раскрыто содержание каждого вопроса; обучающимся не сделаны собственные выводы по теме работы; допущены существенные недостатки в оформлении работы; при защите работы обучающийся демонстрирует владение материалом, но отвечает не на все поставленные вопросы, либо не в достаточно полном объеме;

– «неудовлетворительно» - если проект не выполнена в соответствии с утвержденным планом и заданием, не раскрыто содержание каждого вопроса; обучающимся не сделаны выводы по теме работы, имеются существенные недостатки в оформлении работы; при защите работы обучающийся не демонстрирует владение материалом, не отвечает на поставленные вопросы.

В случае оценивания работы на «неудовлетворительно» работа направляется на дальнейшую доработку.

7. Учебно-методическое и информационное обеспечение дисциплины

7.1. Рекомендуемая основная литература

№	Название
1.	Петров А.А. Компьютерная безопасность. Криптографические методы защиты [Электронный ресурс] / А.А. Петров. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 446 c. — 978-5-4488-0091-7. — Режим доступа: http://www.iprbookshop.ru/63800.html
2.	Бескид П.П. Криптографические методы защиты информации. Часть 1. Основы криптографии [Электронный ресурс] : учебное пособие / П.П. Бескид, Т.М. Тагарникова. — Электрон. текстовые данные. — СПб. : Российский государственный гидрометеорологический университет, 2010. — 95 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/17925.html
3.	Бескид П.П. Криптографические методы защиты информации. Часть 2. Алгоритмы, методы и средства обеспечения конфиденциальности, подлинности и целостности информации [Электронный ресурс] : учебное пособие / П.П. Бескид, Т.М. Тагарникова. — Электрон. текстовые данные. — СПб. : Российский государственный гидрометеорологический университет, 2010. — 104 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/17926.html.

7.2. Рекомендуемая дополнительная литература

№	Название
1.	Калмыков И.А. Криптографические методы защиты информации [Электронный ресурс] : лабораторный практикум / И.А. Калмыков, Д.О. Науменко, Т.А. Гиш. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2015. — 109 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/63099.html
2.	Практикум по выполнению лабораторных работ по дисциплине Криптографические методы защиты информации [Электронный ресурс] / . — Электрон. текстовые данные. — М. : Московский технический университет связи и информатики, 2015. — 67 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/61738.html

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

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

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//*

7.3.1 Программное обеспечение

№ п/п	Наименование	Условия доступа/скачивания
1.	MS Office/ LibreOffice	лицензия университета/ свободное лицензионное соглашение (https://ru.libreoffice.org/)
2.	MS Windows/Arch linux	лицензия университета/ свободное лицензионное соглашение (https://ru.libreoffice.org/)
3.	Visual Studio Community	http://www.visualstudio.com/ru/vs/community
4.	AVG AntiVirus Free	https://www.avg.com/ru-ru/homepage#pc
5.	Avast Free Antivirus	http://avast-anti-virus.ru/?yclid=5762528100398929218
6.	Kaspersky Free	https://www.kaspersky.ru/free-antivirus
7.	360 Total Security	https://www.360totalsecurity.com/ru/

7.3.2 Базы данных, информационно-справочные системы

№ п/п	Наименование программного обеспечения	Условия доступа/скачивания
1.	Гарант	из внутренней сети университета (договор)
2.	Консультант +	
3.	База данных угроз безопасности информации	https://bdu.fstec.ru/

7.4. Рекомендуемые интернет-ресурсы и открытые онлайн курсы.

№ п/п	Наименование	Условия доступа
1.	ISO 27000 Международные стандарты управления информационной безопасностью.	http://iso27000.ru
2.	SecurityLab. Информационный портал по безопасности.	http://www.securitylab.ru
3.	Xgu.ru.	http://xgu.ru/wiki/
4.	Российская Государственная Библиотека	http://www.rsl.ru
5.	Государственная публичная научно-техническая библиотека России	http://www.gpntb.ru
6.	Фундаментальная библиотека Нижегородского государственного университета	http://www.unn.ru/library
7.	Научная библиотека Казанского государственного университета	http://lsl.ksu.ru
8.	Научная электронная библиотека	http://elibrary.ru
9.	Полнотекстовая библиотека учебных и учебно-методических материалов	http://window.edu.ru
10.	Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru

8. 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 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».

Для реализации программы обучения используется лаборатория оснащённая:

специализированным оборудованием по защите информации от утечки по акустическому каналу и по каналу побочных электромагнитных излучений и наводок (Система виброакустического зашумления "СонатаАВ мод.3М"в сост.виброизлучатель пьезоэлектрический ВИ-3М и ПИ-3М,аудиоизлучатель АИ-3М — 1; Устройство защиты "МП-1А" — 1; Устройство защиты объектов информатизации от утечки информации за счет ПЭМИН "Соната-Р" - 1; Фильтр сетевой помехоподавляющий "ФСП-1Ф-7А" - 1);

техническими средствами контроля эффективности защиты информации от утечки по акустическому каналу и каналу побочных электромагнитных излучений и наводок (Устройство поисковое многофункциональное "ST 033" — 1; Комплекс проведения акустических и виброакустических измерений "Спрут-мини-А" - 1; Комплекс обнаружения радиоизлучающих средств и радиомониторинга "Крона" — 1; Имитатор многофункциональный "ИМФ-2" - 1; Прибор-приставка АСК-4106 комбинированный - 1).

9. 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.

10. 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 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. 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: групповая. При групповой форме организации занятий одна и та же работа выполняется бригадами по 2 - 5 человек.

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.

Методические указания обучающимся по выполнению самостоятельной работы

1 Значение самостоятельной работы обучающихся

Самостоятельная работа обучающихся является неотъемлемой частью образовательного процесса. Цель самостоятельной работы – подготовка современного компетентного специалиста и формирование способностей и навыков к непрерывному самообразованию и профессиональному совершенствованию.

Реализация поставленной цели предполагает решение следующих задач:

- качественное освоение теоретического материала по изучаемой дисциплине, углубление и расширение теоретических знаний с целью их применения на уровне межпредметных связей;
- систематизация и закрепление полученных теоретических знаний и практических навыков;
- формирование умений по поиску и использованию нормативной, правовой, справочной и специальной литературы, а также других источников информации;
- развитие познавательных способностей и активности, творческой инициативы, самостоятельности, ответственности и организованности;
- формирование самостоятельности мышления, способностей к саморазвитию, самообразованию, самосовершенствованию и самореализации;
- развитие научно-исследовательских навыков;
- формирование умения решать практические задачи (в профессиональной деятельности), используя приобретенные знания, способности и навыки.

Самостоятельная работа определяется спецификой дисциплины и методикой ее преподавания, временем, предусмотренным учебным планом, а также ступенью обучения, на которой изучается дисциплина. Основными формами организации самостоятельной работы студентов являются: аудиторная самостоятельная работа под руководством и контролем преподавателя (на лекциях, практических занятиях и консультациях); внеаудиторная самостоятельная работа под руководством и контролем преподавателя (на консультациях, при проведении научно-исследовательской работы), внеаудиторная самостоятельная работа без непосредственного участия преподавателя (подготовка к аудиторным занятиям, олимпиадам, конференциям, выполнение контрольных работ, работа с электронными информационными ресурсами, подготовка к экзаменам и зачетам). Самостоятельная работа студентов обеспечивается настоящими методическими рекомендациями.

Самостоятельная работа обучающихся по курсу «Криптографические методы защиты информации» - необходимая составляющая подготовки специалиста в области информационной безопасности.

Внеаудиторная самостоятельная работа – планируемая учебная, учебно-исследовательская, научно-исследовательская работа обучающихся, выполняемая во внеаудиторное время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия. Целью самостоятельной работы обучающихся является овладение фундаментальными знаниями методов криптографии, профессиональными умениями и навыками, опытом творческой, исследовательской деятельности.

2 Общие рекомендации по организации самостоятельной работы обучающихся

Дисциплина «Криптографические методы защиты информации» позволяет привить обучающимся навыки применения базовых знаний языков программирования в криптографии. Также обучающиеся должны опираться, в основном, на знания и умения, полученные на лекционных и практических занятиях. Это дает необходимый базис для дальнейшего углубленного изучения других дисциплин. Однако эти знания необходимо активизировать.

Формы самостоятельных работ обучающихся, предусмотренные дисциплиной:

- Подготовка к лабораторным занятиям;

- Самостоятельное изучение учебных вопросов;
- Выполнение расчётно-графической работы;
- Подготовка к экзамену.

Для самостоятельной подготовки к лабораторным занятиям, изучения учебных вопросов, подготовки к экзамену можно рекомендовать следующие источники:

- конспекты лекций и материалы практических занятий;
- учебную литературу соответствующего профиля.

Преподаватель в начале чтения курса информирует студентов о формах, видах и содержании самостоятельной работы, разъясняет требования, предъявляемые к результатам самостоятельной работы, а также формы и методы контроля и критерии оценки.

3 Методические рекомендации по подготовке к практическим занятиям

Практическое занятие – это одна из форм учебной работы, которая ориентирована на закрепление изученного теоретического материала, его более глубокое усвоение и формирование умения применять теоретические знания в практических, прикладных целях. Особое внимание на практических занятиях уделяется выработке учебных или профессиональных навыков. Такие навыки формируются в процессе выполнения конкретных заданий – упражнений, задач и т. п. – под руководством и контролем преподавателя. Ведущей целью практических занятий является формирование умений и приобретение практического опыта, направленных на формирование профессиональных компетенций (способности выполнять определенные действия, операции, необходимые в профессиональной деятельности) или общих компетенций (общие компетенции необходимы для успешной деятельности как в профессиональной, так и во внепрофессиональной сферах).

Содержанием практических занятий являются решение разного рода задач, в том числе профессиональных (анализ производственных ситуаций, решение ситуационных производственных задач, выполнение профессиональных функций в деловых играх и т.п.), выполнение вычислений, расчетов, чертежей, работа с измерительными приборами, оборудованием, аппаратурой, работа с нормативными документами, инструктивными материалами, справочниками, составление проектной, плановой и другой технической и специальной документации и другое.

4 Методические рекомендации по подготовке к лабораторным занятиям

Ведущая дидактическая цель лабораторных работ–закрепление на практике умения проектировать и программировать микропроцессорные системы. Лабораторные работы и практические занятия могут носить репродуктивный, частично - поисковый и поисковый характер.

Работы, носящие репродуктивный характер, отличаются тем, что при их проведении студенты пользуются подробными инструкциями, в которых указаны: цель работы, пояснения (теория, основные характеристики), оборудование, аппаратура, материалы и их характеристики, порядок выполнения работы, таблицы, выводы (без формулировки), контрольные вопросы, учебная и специальная литература.

Работы, носящие частично - поисковый характер, отличаются тем, что при их проведении студенты не пользуются подробными инструкциями, им не дан порядок выполнения необходимых действий, и требуют от студентов самостоятельного подбора оборудования, выбора способов выполнения работы в инструктивной и справочной литературы и др.

Работы, носящие поисковый характер, характеризуются тем, что студенты должны решить новую для них проблему, опираясь на имеющиеся у них теоретические знания.

Формы организации студентов на лабораторных работах и практических занятиях: фронтальная, групповая и индивидуальная.

При фронтальной форме организации занятий все студенты выполняют одновременно одну и ту же работу.

При групповой форме организации занятий одна и та же работа выполняется бригадами по 2 - 5 человек.

При индивидуальной форме организации занятий каждый студент выполняет индивидуальное задание.

Оформление письменного отчета по выполненной работе в соответствии с требованиями. Письменный отчет о выполненной лабораторной работе должен содержать следующие сведения:

- название работы и сведения об авторе отчета (курс, имя, фамилия);
- цель работы и формулировка используемого метода анализа;
- описание выполнения лабораторных исследований или расчетов;
- список используемой литературы.

Оценки за выполнение лабораторных работ учитывается как показатель текущей успеваемости обучающегося.

5 Методические рекомендации по самостоятельному изучению учебных вопросов

Темы, вынесенные на самостоятельное изучение, необходимо законспектировать. В конспекте кратко излагается основная сущность учебного материала, приводятся необходимые обоснования, табличные данные, схемы, эскизы, расчеты и т.п. Конспект целесообразно составлять целиком на тему. При этом имеется возможность всегда дополнять составленный конспект вырезками и выписками из журналов, газет, статей, новых учебников, брошюр по обмену опытом, данных из Интернета и других источников. Таким образом, конспект становится сборником необходимых материалов, куда студент вносит всё новое, что он изучил, узнал. Такие конспекты представляют, большую ценность при подготовке к занятиям.

Основные этапы самостоятельного изучения учебных вопросов:

1. Первичное ознакомление с материалом изучаемой темы по тексту учебника, картам, дополнительной литературе.
2. Выделение главного в изучаемом материале, составление обычных кратких записей.
3. Подбор к данному тексту опорных сигналов в виде отдельных слов, определённых знаков, графиков, рисунков.
4. Продумывание схематического способа кодирования знаний, использование различного шрифта и т.д.
5. Составление опорного конспекта.

6 Методические рекомендации по подготовке к зачету

Подготовка студентов к сдаче зачета включает в себя:

- просмотр программы учебного курса;
- определение необходимых для подготовки источников (учебников, дополнительной литературы и т. д.) и их изучение;
- использование конспектов лекций, материалов практических занятий;
- консультирование у преподавателя.

Подготовка к зачету начинается с первого занятия по дисциплине, на котором студенты получают общую установку преподавателя и перечень основных требований к текущей и итоговой отчетности. При этом важно с самого начала планомерно осваивать материал, руководствуясь, прежде всего перечнем вопросов к зачету (экзамену), конспектировать важные для решения учебных задач источники. В течение семестра происходят пополнение, систематизация и корректировка студенческих наработок, освоение нового и закрепление уже изученного материала.

7 Методические рекомендации по подготовке к экзамену

Экзамен преследует цель оценить работу студента за определенный курс: полученные теоретические знания, их прочность, развитие логического и творческого мышления, приобретение навыков самостоятельной работы, умения анализировать и синтезировать полученные знания и применять на практике решение практических задач.

Экзамен проводится в письменной форме по билетам, утвержденным заведующим кафедрой. Экзаменационный билет включает в себя два вопроса и задачи. Формулировка вопросов совпадает с формулировкой перечня вопросов, доведенного до сведения студентов за один месяц до экзаменационной сессии. В процессе подготовки к экзамену организована предэкзаменационная консультация для всех учебных групп. Результат экзамена выражается оценкой «отлично», «хорошо», «удовлетворительно».

С целью уточнения оценки экзаменатор может задать не более одного-двух дополнительных вопросов, не выходящих за рамки требований рабочей программы. Под дополнительным вопросом подразумевается вопрос, не связанный с тематикой вопросов билета. Дополнительный вопрос, также, как и основные вопросы билета, требует развернутого ответа. Кроме того, преподаватель может задать ряд уточняющих и наводящих вопросов, связанных с тематикой основных вопросов билета. Число уточняющих и наводящих вопросов не ограничено.

8 Методические рекомендации по оформлению курсового проекта

Курсовой проект – одна из форм текущей аттестации знаний, полученных обучающимися при самостоятельном изучении нормативного материала и научной литературы. Он представляет собой, с одной стороны, мини научную работу, предполагающую творческое изложение результатов осмысления теоретических и практических проблем. С другой стороны, способ контроля со стороны преподавателя за самостоятельной работой обучающихся.

Основными целями и задачами являются:

- углубление знаний обучающихся по отдельному вопросу или теме;
- развитие умения анализировать теоретический и практический материал;
- формирование умения в письменном виде логично и последовательно излагать свои мысли.

Основные этапы:

- выбор темы, ее согласование с научным руководителем;
- подбор необходимой литературы и разработка плана работы;
- изучение и обработка литературы;
- сбор статистических данных, их анализ и обобщение;
- написание проекта по главам, передача их научному руководителю на проверку;
- доработка отдельных частей курсового проекта с учетом требований и замечаний научного руководителя;
- завершение и оформление курсового проекта в соответствии с требованиями стандарта и настоящих методических указаний;
- сдача курсового проекта научному руководителю для оформления допуска к защите;
- защита курсового проекта.

Структура курсового проекта:

1. Титульный лист.
2. Оглавление.
3. Введение.
4. Основная часть (разделы, подразделы, пункты).
5. Заключение.

6. Список использованных источников.

7. Приложение.

Оформление курсового проекта, включая титульный лист (обложку), производится по установленному образцу, который размещен на сайте факультета и кафедры. На титульном листе студент указывает название кафедры, темы, свою фамилию и инициалы, номер учебной группы, а также должность, научное звание руководителя.

При составлении плана обучающимся необходимо учесть, что ими должны быть рассмотрены теоретико-методологические и практические аспекты исследуемой темы. В случае необходимости план может корректироваться по согласованию с научным руководителем, в чью компетенцию входит утверждение отдельных разделов и подразделов плана.

Введения должен составлять 2-3 страницы и включать:

- обоснование актуальности выбранной темы, т. е. степень ее значимости в данный момент и в данной ситуации для определенных субъектов;
- определение цели и задач исследования. Цель работы должна быть сформулирована четко и лаконично, соответствовать выбранной теме исследования и направленной на достижение результатов. Поставленные задачи должны уточнять цель, конкретизировать ее, соответствовать разделам и подразделам плана;
- характеристику теоретической и методологической базы исследования;
- описание объекта исследования, представляет собой краткую характеристику социально-экономического процесса или явления, создавшего проблемную ситуацию, исследуемую в работе;
- краткий аналитический обзор использованной литературы по теме. Обзор литературы должен показать умение студента систематизировать источники, критически их рассматривать, выделять существенное и определять главное в современном состоянии изученности темы;
- перечень использованной информационной базы по теме исследования. Необходимо перечислить источники получения статистических и аналитических материалов, документы законодательных и исполнительных органов власти; данные, опубликованные в периодических изданиях.

В том случае, если в работе имеется обоснование нового подхода к решению поставленной проблемы, которое сделано самостоятельно студентом, во введении необходимо это указать.

Первый раздел посвящается анализу теоретических аспектов темы, анализу проблемной ситуации. Первый раздел (теоретическая часть) представляет собой анализ различных теоретических взглядов российских и зарубежных исследователей по теме курсовой работы. При рассмотрении каждого направления необходимо делать ссылку на его автора и источник, где данные идеи нашли отражение. Здесь же необходимо дать определения основных понятий темы, показать подходы различных авторов к трактовке их сущности.

Второй раздел курсового проекта, который также начинается с нового листа, являясь логическим продолжением первого раздела, должен служить своеобразной иллюстрацией практической реализации изученных теоретических подходов по теме исследования. В нем описываются математические основы моделирования, анализа и прогнозирования изучаемого объекта или явления.

В третьем разделе описываются результаты моделирования и прогнозирования изучаемого объекта, излагаются вопросы, посвященные путям совершенствования или решения проблем в изучаемых явлениях и процессах. Здесь необходимо проанализировать связи исследуемой проблемы с социальными проблемами. В данном разделе необходимо использовать статистические данные или другой фактический материал, отражающий объективную реальность практической деятельности хозяйствующих субъектов. Фактические данные, цифровую информацию следует обработать, сгруппировать,

поместить в таблицы, провести их анализ, определить процентные соотношения, сопоставить и описать. На их основе составляются графики, диаграммы, схемы, с помощью которых можно проиллюстрировать изложенный материал.

Каждый раздел может включать 2-4 подраздела, логически связанных между собой и уточняющих друг друга.

Итоговым разделом курсового проекта является заключение, которое также начинается с нового листа. Заключение представляет собой выводы, сделанные самостоятельно студентом, по каждому из написанных разделов курсового проекта. Объем заключения 2-4 страницы.

Список использованных источников должен включать только те источники, которые были проработаны при выполнении курсового проекта и на которые имеются ссылки в тексте работы. Данный список должен включать не менее 15-20 литературных источников, в том числе действующие законодательные акты, регулирующие экономические отношения по исследуемой проблеме, решения правительства, статистические справочники, монографии, публикации в периодической печати и другие материалы. Список источников должен быть оформлен в соответствии со стандартом. Рекомендуется при изучении той или иной статьи, монографии, статистических данных сразу же выписывать полное их наименование и указывать страницу, если есть ссылка на данный источник в тексте работы.

Литературу в списке располагают в алфавитном порядке, не нарушая ее нумерации, но, соблюдая при этом следующую последовательность:

а) нормативно-правовые акты:
законы и постановления правительства РФ;
указы Президента РФ;
законодательные акты Федерального собрания РФ;
инструкции, распоряжения Министерств и ведомств РФ;
б) книги (монографии, сборники);
в) периодические издания,
г) статистические сборники и справочники;
д) Интернет-ресурсы;
е) печатные материалы на иностранных языках.

Приложения необходимы в том случае, если в курсовой работе использована большая по объему информация, на основе которой были сделаны таблицы, построены графики, диаграммы, содержащиеся в тексте внутри разделов и подразделов работы. В этом случае исходная информация в виде таблиц или иных документов помещается в Приложения в порядке использования этих данных в тексте работы.

Требования по оформлению курсового проекта:

Рекомендованный объем работы – 25-30 листов напечатанных на компьютере страниц без учета оглавления, списка использованных источников и приложения.

Текст рукописи печатается шрифтом Times New Roman, кегль 14 pt, с интервалом - 1,5.

Поля: слева - 3 см, справа – 1,5 см, сверху и снизу - 2 см.

Красная строка - 1,25 см, меж- абзацный интервал – 0.

Форматирование основного текста и ссылок – в параметре «по ширине».

Название «Оглавление», «Введение», «Заключение», «Приложение», «Литература», а также заголовки глав и параграфов выделяются одинаковым темным, полужирным шрифтом.

Цитаты в тексте оформляются в виде сносок в конце страницы.

Иллюстрации (графики, схемы, диаграммы) могут быть в основном тексте и в разделе приложений. Все иллюстрации именуются рисунками. Все рисунки, таблицы и

формулы нумеруются арабскими цифрами и имеют сквозную нумерацию в пределах главы или приложения. Все иллюстрации должны иметь подпись.

Нумеровать страницы следует по книжному варианту: печатными цифрами, в нижнем правом углу страницы, начиная с текста «Введения» (с. 3). Работа имеет сквозную нумерацию до последней страницы. В оглавлении указываются начальные страницы всех частей и параграфов работы (название главы отдельной страницы не имеет), кроме списка литературы и приложений (в тексте нумеруются).Пишется слово «глава», главы нумеруются римскими цифрами, параграфы - арабскими, знак не пишется; части работы «Введение», «Заключение», «Литература» нумерации не имеют.

Названия глав и параграфов пишутся с красной строки. Заголовки «Введение», «Заключение», «Литература» пишутся посередине, вверху листа, без кавычек, точка не ставится.

Объем введения и заключения работы - 1,5-2 страницы печатного текста.

Работа должна быть прошита.

В работе используются три вида шрифта: 1 - для выделения названий глав, заголовков «Оглавление», «Литература», «Введение», «Заключение»; 2 - для выделения названий параграфов; 3 - для текстовки.

Курсовой проект предполагает защиту в форме публичного выступления или индивидуального собеседования.

Итоговая оценка за курсовой проект складывается:

1) из оценивания научным руководителем объема изученной литературы;
2) из оценивания представленного письменного текста с точки зрения его содержания (раскрытие темы, самостоятельность исследования, творческие выводы, анализ практики) и оформления;
3) из оценивания защитной речи и ответов на вопросы по теме работы.

Методические рекомендации преподавателю по проведению занятий

Общие положения.

Основу профессиональной деятельности преподавателя составляет его методическая деятельность – деятельность по организации педагогического процесса, направленная на полноценно результативное освоение обучающимися соответствующего учебного предмета. Овладение преподавателем методической деятельностью происходит как в рамках методической подготовки в вузе и учреждениях дополнительного профессионального образования, так и в процессе самообразования. Уровень методической деятельности преподавателя должен быть таким, чтобы он мог помочь студентам быть активными деятелями в постижении знаний и в самосовершенствовании учебной деятельности. Поэтому высокие требования, предъявляемые к уровню методической деятельности преподавателей, автоматически выдвигают высокие требования к организации методической подготовки в вузе, в системе повышения квалификации и переподготовки и к процессу самообразования.

В современных условиях повышение уровня методической подготовки преподавателя может обеспечиваться определением и разработкой новых подходов к целям, содержанию и организации методической подготовки.

Основными требованиями, которые предъявляются в современных условиях к преподавателю математики в вузе являются:

1. Высокий уровень профессиональной математической подготовки, предполагающий знание программы по математике в полном объёме, умение соблюдать преемственность в преподавании математики.
2. Владение современным дидактическим инструментарием, позволяющим успешно работать с группой обучаемых, имеющих различный уровень базовой подготовки.

3. Умение осуществлять в учебном процессе дифференцированный, личностно-ориентированный подход к студентам.

4. Знание современных ИТ и их возможностей в области математики; умение квалифицированно оценивать и отбирать программные продукты с точки зрения их педагогической целесообразности для использования в учебном процессе.

5. Наличие представлений о специфике смежных дисциплин учебной программы для установления и укрепления межпредметных связей.

6. Умение организовывать самостоятельную работу обучаемых при изучении математики.

В основе организации обучения студентов лежит принцип методической поддержки, который требует, чтобы студенты были в достаточной мере обеспечены учебно-методической литературой, позволяющей освоить базовый уровень подготовки.

Критерием реализации принципа методической поддержки служит наличие в учебно-методической литературе материалов следующих видов:

- ориентирующие учебно-методические материалы – тексты, раскрывающие технологии конструирования методической деятельности преподавателя и удовлетворяющие требованиям обоснованности, технологичности, минимальности;

- примеры-образцы методических разработок, которые демонстрируют реализацию ориентировочных основ методической деятельности и удовлетворяют требованиям научности содержания, методов и средств обучения, связи обучения с жизнью каждого учащегося, выдвижения учащихся на ведущие позиции;

- учебно-методические материалы для самоконтроля преподавателя – материалы, позволяющие осуществлять самоконтроль собственных методических разработок и выполнения методических знаний;

- целевые учебно-методические тексты – тексты, раскрывающие цели представленных учебно-методических материалов;

- методические задания, удовлетворяющие следующим требованиям: разработаны на основе анализа практики преподавателей (требование практического обобщения); учитывают те методические вопросы, в решении которых большинство преподавателей испытывают методические трудности (требование методических трудностей); снабжены методической поддержкой, обеспечивающей успешность их выполнения (требование успешности выполнения); являются комплексными (требование комплексности).

Лекционно-практическая форма обучения объективно предполагает разработку специальных методических пособий для проведения как лекций, так и для практических занятий. Упрощённо говоря, в основе любой методики лежат два основных компонента – содержание обучения («чему учить») и способы обучения («как учить»). Естественно, при формировании частных методик следует учитывать много субъективных факторов, связанных со специализацией студентов, уровнем их базовой подготовки, объёмом аудиторной нагрузки и т.д.

Задачи, которые решаются в ходе практических занятий должны:

1) расширять и закреплять теоретические знания, полученные в ходе лекционных занятий;

2) формировать у студентов практические умения и навыки, необходимые для успешного решения задач;

3) развивать у студентов потребность в самообразовании и совершенствовании знаний и умений в процессе изучения дисциплины;

4) формировать творческое отношение и исследовательский подход в процессе изучения;

5) формировать профессионально-значимых качеств будущего специалиста и навыков приложения полученных знаний в профессиональной сфере.

Разрабатывая методическое пособие для проведения практических занятий, в первую очередь необходимо опираться на действующую рабочую программу по

дисциплине, в которой обязательно должны быть определены количество и тематика практических занятий на каждый семестр. Для каждого занятия определяются тема, цель, структура и содержание. Исходя из них, выбираются форма проведения занятия (комбинированная, самостоятельная работа, фронтальный опрос, тестирование и т.д.) и дидактические методы, которые при этом применяет преподаватель (индивидуальная работа, работа по группам, деловая игра и проч.). Целесообразность выбора преподавателем того или иного метода зависит, главным образом, от его эффективности в конкретной ситуации. Например, если преподаватель ставит задачу проверки уровня усвоения теоретического материала лекции, предшествующей данному практическому занятию, то удобно провести в начале занятия устный фронтальный опрос; если ставится задача проверить знания студентов по более широкому кругу вопросов, то целесообразно провести небольшое по времени (не более, чем на 1 академический час) тестирование; для выработки навыков решения обычно проводят письменный опрос студентов у доски и т.д.

Особое внимание следует уделить хронометражу занятия, т.е. выделению на каждый этап занятия определённого времени. Для преподавателя, особенно начинающего, чрезвычайно важно придерживаться запланированного хронометража. Если этого не удаётся сделать, то преподавателю необходимо проанализировать ход занятия и, возможно, внести изменения либо в его структуру, либо в форму его проведения.

Обучение студентов на первых практических занятиях должно носить выраженный дифференцированный характер в зависимости от уровня и состояния их предшествующей подготовки.

Решение учебных задач является универсальным видом учебной деятельности, который успешно применяется в методике всех вузовских дисциплин. С его помощью решаются разнообразные дидактические задачи, отражающие специфику целей, форм и методов обучения. Следует учитывать тот факт, что к изучению некоторых дисциплин приступают уже в определённой мере подготовленными в результате предшествующей школьной подготовки, и это следует учитывать при составлении и проведении соответствующих практических работ. Поэтому здесь можно представить задание в более сложном, формализованном виде, не сопровождая его чрезмерно подробными инструкциями по выполнению - достаточно будет привести несколько типичных несложных примеров. С другой стороны, для того, чтобы успешно решать принципиально новые для них задачи, студенты обязательно должны разбирать типовые способы их решения не только на лекциях, но и на практических занятиях. При этом, однако, преподаватель не должен превращать практическое занятие в продолжение лекции.

Чтобы научить студентов применять на практике теоретические знания, полученные при изучении математики преподаватель должен уметь выбирать или разрабатывать необходимый математический учебный материал для каждого занятия. Необходимость планировать и анализировать учебно-воспитательный процесс в дидактическом, психологическом, методическом аспектах с учетом современных требований к преподаванию математики обуславливает, в свою очередь, необходимость обоснованного выбора эффективных методов, форм и средств обучения, контроля результатов усвоения студентами программного материала.

Преподаватель должен систематически проводить самоанализ, самооценку и корректировку собственной деятельности на уроках и внеклассных занятиях по математике, разрабатывать и проводить диагностику для определения уровня знаний и умений студентов, разрабатывать и реализовывать программы для индивидуальных и групповых форм работы с учетом математических способностей студентов.