МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Факультет математики и компьютерных наук

УТВЕРЖДАЮ:
Проректор по учебной работе, качеству образования – первый проректор
_____ Хагуров Т.А.
подпись
«27» мая 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.В.ДВ.01.02 КРИПТОГРАФИЯ И ЗАЩИТА ИНФОРМАЦИИ

Специальность 01.05.01 Фундаментальные математика и механика

Направленность (профиль) Фундаментальная математика и ее приложения,

Форма обучения Очная

Квалификация Математик. Механик. Преподаватель

Краснодар 2022

Рабочая программа дисциплины Криптография и защита информации составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по специальности 01.05.01 Фундаментальные математика и механика

Программу составил(и):
А.В. Рожков, профессор, д.ф.-м.н., профессор _____

Рабочая программа дисциплины криптография и защита информации утверждена на заседании кафедры функционального анализа и алгебры
протокол № 9 «13» апреля 2022 г.
Заведующий кафедрой функционального анализа и алгебры
Барсукова В.Ю. _____

Утверждена на заседании учебно-методической комиссии факультета математики и компьютерных наук
протокол № 5 «5» мая 2022 г.
Председатель УМК факультета Шмалько С.П. _____

Рецензенты:
Наумова Н.А., доктор технических наук, профессор кафедры прикладной математики ФГБОУ ВО «Кубанский государственный технологический университет»
Иванисова О.В., кандидат физико-математических наук, доцент кафедры ВМИ КубГУ

1 Цели и задачи изучения дисциплины.

1.1 Цель освоения дисциплины.

Цель освоения дисциплины – рассмотрение задач информатизации и программно-аппаратных основ кодирования информации. Изучение этой дисциплины является важной составной частью современного математического образования и образования в области компьютерных наук.

1.2 Задачи дисциплины.

Задачи освоения дисциплины «Криптография и защита информации»: Получение базовых теоретических и практических сведений и навыков о структуре и алгоритмах кодирования информации. Математических основ анализа каналов связи с шумом. Основ теории кодов, исправляющих ошибки. Основ теории информации. Прежде всего алгебраических, связанных с вычислительными и числовыми вопросами алгебры и криптографии. Применение этих знаний на практике, при рассмотрении перспектив развития математических и компьютерных наук, месте и роли вычислительных приемов и методов, при решении вопросов защиты информации.

Изучение теоретических основ предмета: Информационные объекты. Компьютерная алгебра и численный анализ информационных систем. Коды Хэмминга. Теория информации по Шеннону. Алгоритмы кодирования информации жестких и съемных дисков.

1.3 Место дисциплины (модуля) в структуре образовательной программы.

Дисциплина «Криптография и защита информации» относится к части, формируемой участниками образовательных отношений Блока 1 "Дисциплины (модули)" учебного плана и является дисциплиной по выбору Б1.В.ДВ.01.02.

Данная дисциплина, как алгоритмическая основа криптографии, призвана содействовать фундаментализации образования, укреплению правосознания и развитию системного мышления студентов. А также развитию навыков применения современных компьютерных средств для решения естественно-научных проблем.

1.4 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих компетенций:

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине (знает, умеет, владеет (навыки и/или опыт деятельности))
ПК-4. Способен разрабатывать программное обеспечение для решения прикладных задач в сфере профессиональной деятельности	
ПК-4.1 Имеет навыки использования современных языков программирования для разработки программного обеспечения ПК-4.2 Знает стандартные решения, библиотеки программных модулей, шаблоны, классы объектов, используемые при разработке прикладного программного обеспечения. ПК-4.3 Применяет методы и средства проектирования программного обеспечения, структур данных, баз данных, программных интерфейсов ПК-4.4 Ориентируется в современных алгоритмах компьютерной математики и имеет практический опыт разработки программных модулей на основе механико-математических моделей ПК-4.5 Способен внедрять результаты математических исследований и разработок прикладного	Знать: об основных задачах и понятиях криптографии; о видах информации, подлежащей кодированию; о классификации шифров; о методах защиты компьютерных систем и сетей. Уметь использовать: шифры; линейные коды; циклические коды; основные математические методы, используемые в анализе типовых алгоритмов. Владеть: алгоритмами решение систем линейных уравнений по разным модулям; методами построения генераторов псевдослучайных последовательностей; алгоритмами построения шифров

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине (знает, умеет, владеет (навыки и/или опыт деятельности))
программного обеспечения в соответствии с установленными требованиями	

Результаты обучения по дисциплине достигаются в рамках осуществления всех видов контактной и самостоятельной работы обучающихся в соответствии с утвержденным учебным планом.

Индикаторы достижения компетенций считаются сформированными при достижении соответствующих им результатов обучения.

2. Структура и содержание дисциплины.

2.1 Распределение трудоёмкости дисциплины по видам работ.

Общая трудоёмкость дисциплины составляет 2 зач. ед. (72 часа), их распределение по видам работ представлено в таблице.

Вид учебной работы		Всего часов	Семестры (часы)			
			7			
Контактная работа, в том числе:						
Аудиторные занятия (всего):		**18**	**18**			
Занятия лекционного типа				-	-	-
Лабораторные занятия		18	18	-	-	-
Занятия семинарского типа (семинары, практические занятия)				-	-	-
Иная контактная работа:						
Контроль самостоятельной работы (КСР)		4	4			
Промежуточная аттестация (ИКР)		0,2	0,2			
Самостоятельная работа, в том числе:		**49.8**	**49.8**			
Курсовая работа		-	-	-	-	-
Проработка учебного (теоретического) материала		14	14	-	-	-
Выполнение индивидуальных заданий (подготовка сообщений, презентаций)		12	12	-	-	-
Реферат		4	4	-	-	-
Подготовка к текущему контролю		19,8	19,8	-	-	-
Контроль:						
Подготовка к экзамену		-	-			
Общая трудоемкость	**час.**	**72**	**72**	**-**	**-**	**-**
	в том числе контактная работа	**22,2**	**22,2**			
	зач. ед	**2**	**2**			

2.2 Структура дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы дисциплины, изучаемые в 7 семестре *(очная форма)*

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1	Основные понятия и определения теории кодирования.	14			4	10
2	Свойства энтропии. Теорема Шеннона для кодирования в двоичном симметричном канале связи с шумом.	14			4	10
3	Алгебраические методы в теории кодов.	14			4	10
4	Теория кодов и криптография.	25.8			6	19.8
	Итого по дисциплине:				18	49.8

Примечание: Л – лекции, ПЗ – практические занятия / семинары, ЛР – лабораторные занятия, СРС – самостоятельная работа студента

2.3 Содержание разделов дисциплины:

2.3.1 Занятия лекционного типа.

Не предусмотрены

2.3.2 Занятия семинарского типа.

Не предусмотрены

2.3.3 Лабораторные занятия.

№	Наименование лабораторных работ	Форма текущего контроля
1	3	4
1	Двоичный симметричный канал связи. Линейные коды. Границы объемов кодов. Код Хэмминга и его свойства. Способы построения новых кодов.	Р
2	Декодирование двоичных кодов. Декодирование линейного кода. Вероятность ошибки декодирования. Хеммингово расстояние, Хемминговы сферы и корректирующая способность..	Р
3	Двоичные коды Рида-Маллера. Групповые коды. Функция Эйлера и Мебиуса. Группы обратимых элементов в кольцах.	Э
4	Структура мультипликативной группы кольца вычетов. Обратимые элементы. Примитивные элементы. Коды Васильева.	Р
5	Поля Галуа, неприводимые многочлены. Псевдослучайные последовательности. Сложность и скорость выполнения алгоритмов.	Р
6	Порождающий и проверочный полиномы. Порождающий многочлен. Кодирование и декодирование двоичных циклических кодов	Э
7	Рекурсивные систематические сверточные коды. Свободное расстояние. Связь с блоковыми кодами. Декодирование: Алгоритм Витерби в Хеммингoвой метрике.	Р

8	Декодирование по максимуму правдоподобия и метрики. Криптографические алгоритмы и протоколы. Блочные и поточные шифры. Однонаправленные функции. Сетевое кодирование и шифрование. Понятие о стеганографии.	Р

Защита лабораторной работы (ЛР), выполнение курсового проекта (КП), курсовой работы (КР), расчетно-графического задания (РГЗ), написание реферата (Р), эссе (Э), коллоквиум (К), тестирование (Т).

2.3.4 Примерная тематика курсовых работ (проектов)

Курсовые работы не предусмотрены.

2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
1	Подготовка рефератов и научных сообщений	Рожков А.В. «Темы исследовательских работ и методические указания по их написанию», утвержденные кафедрой функционального анализа и алгебры, протокол № 9 «13» апреля 2022 г.
2	Решение задач	Рожков А.В. «Лабораторная работа по теоретико-числовым методам криптографии по криптографии. Методические указания», утвержденные кафедрой функционального анализа и алгебры, протокол № 9 «132» апреля 2022 г.
3	Самостоятельное освоение теории	Рожков А.В. «Теоретико-числовые методы криптографии. Учебное пособие», утвержденное кафедрой функционального анализа и алгебры, протокол № 9 «132» апреля 20229 .

1. Методические указания для подготовки к занятиям лекционного и семинарского типа. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5 от 05 мая 2022 г.

2. Методические указания по выполнению самостоятельной работы обучающихся. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5 от 05 мая 2022 г.

3. Методические указания по использованию интерактивных методов обучения. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5т от 05 мая 2022 г.

4. Методические указания по подготовке эссе, рефератов, курсовых работ. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5т от 05 мая 2022 г.

5. Методические указания по выполнению лабораторных работ. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5 от 05 мая 2022 г.

6. Методические указания по выполнению расчетно-графических заданий. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5 от 05 мая 2022 г.

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:
– в печатной форме с увеличенным шрифтом,
– в форме электронного документа.
Для лиц с нарушениями слуха:
– в печатной форме,
– в форме электронного документа.
Для лиц с нарушениями опорно-двигательного аппарата:
– в печатной форме,
– в форме электронного документа,

3. Образовательные технологии.

Активные и интерактивные формы, лекции, контрольные работы, реферативные доклады (по некоторым темам в виде презентации) и зачет. В течение семестра студенты решают задачи, указанные преподавателем, к каждому лабораторному занятию. Каждый студент готовит реферативный доклад по одной из ниже научных тем. Зачет выставляется после выполнения определенного количества (практических и теоретических) заданий контрольных работ и отчета по реферативному докладу. В случае невыполнения какого-то из приведенных требований, студенту для сдачи зачета предлагаются по усмотрению преподавателя некоторые практические и теоретические задания, подобные предложенным ниже.

К образовательным технологиям также относятся интерактивные методы обучения.

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций со студентом при помощи электронной информационно-образовательной среды ВУЗа.

В рамках реализации компетентностного подхода предусматриваются следующие основные виды активных и интерактивных форм проведения учебных занятий, которые указываются в рабочих программах дисциплин, профессиональных модулей, практик в рамках которых они реализуются:

– применение электронных образовательных ресурсов;

– компьютерные симуляции;

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации.

аттестации

Структура оценочных средств для текущей и промежуточной аттестации

№ п/п	Код и наименование индикатора (в соответствии с п. 1.4)	Результаты обучения (в соответствии с п. 1.4)	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
1	ПК-4.1 Понимает и объясняет место преподаваемо-го предмета в структуре учебной деятельности; возможности предмета по формированию УУД; специальные приемы вовлечения в учебную деятельность по предмету обучающихся с разными образовательными потребностями; устанавливать контакты с обучающимися разного возраста и их родителями (законными представителями), другими педагогическими и иными работниками; современные педагогические технологии реализации компетентностного подхода с учетом возрастных и индивидуальных особенностей обучающихся; методы и	Знать: о целях, задачах, принципах и основных направлениях обеспечения информационной безопасности государства; о методологии создания систем защиты информации;	Контрольная работа №1- Значение информационной безопасности для субъектов информационных отношений.	1.Сущность и понятие информационной безопасности. 2.Значение информационной безопасности для субъектов информационных отношений. 3.Место информационной безопасности в системе национальной безопасности.

	технологии поликультурного, дифференцированного и развивающего обучения			
2	ПК-4.2 Осуществляет выбор места преподаваемого предмета в структуре учебной деятельности; воз-можности предмета по формированию УУД; специальных приемов вовлечения в учебную деятель-ность по предмету обучающихся с разными образо-вательными потребностями; устанавливает контакты с обучающимися разного возраста и их родителями (законными представителями), другими педагогическими и иными работниками; современных педагогических технологий реализации компетент-ностного подхода с учетом возрастных и индивиду-альных особенностей обучающихся; методов и тех-нологий поликультурного, дифференцированного и развивающего	Уметь: выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации;	Вопросы для устного (письменного) опроса по теме, разделу Источники, виды и методы дестабилизирующего воздействия на защищаемую информацию.	4.Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности. 5. Источники, виды и методы дестабилизирующего воздействия на защищаемую информацию. 6. Каналы и методы несанкционированного доступа к конфиденциальной информации.

Контрольная работа

Вариант 1

Применения и разработки шифровальных средств ……

Вариант 2

Применения электронной подписи.…….

Вариант 3

Модели, стратегии и системы обеспечения информационной безопасности.

Вариант 4

Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.

Вариант 5

Компьютерная система как объект информационной безопасности.

Список теоретических вопросов (для самостоятельных работ и зачета)

1. Защита персональных данных.
2. История криптографии; классические шифры, шифры гаммирования.
3. Принципы построения криптографических алгоритмов.
4. Различие между программными и аппаратными реализациями шифров.
5. Функция Эйлера и Мебиуса.
6. Группы обратимых элементов в кольцах.
7. Структура мультипликативной группы кольца вычетов.
8. Обратимые элементы.
9. Примитивные элементы.
10. Особенности использования вычислительной техники в криптографии вопросы организации сетей засекреченной связи.
11. Криптографические хеш-функции.
12. Электронная подпись.
13. Криптографические протоколы.
14. Предмет и задачи программно-аппаратной защиты информации.
15. Идентификация субъекта, понятие протокола идентификации.
16. Пароли и ключи, организация хранения ключей.

4.1 Фонд оценочных средств для проведения текущего контроля.

Список теоретических вопросов (для подготовки к зачету)

17. Евклидовы кольца.
18. Кольца вычетов.

19. Функция Эйлера.
20. Функция Мебиуса.
21. Теорема Ферма.
22. Китайская теорема об остатках.
23. Однонаправленные функции.
24. Сложность разложения на множители.
25. Конечные поля.
26. Алгоритм извлечения квадратных корней в конечном поле.
27. Неприводимые многочлены над полями Галуа.
28. Период многочлена.
29. Решение систем линейных уравнений по разным модулям.
30. Генераторы псевдослучайных последовательностей.
31. Определение кода, исправляющего ошибки.
32. Расстояние Хэмминга.
33. Коды Хэмминга.
34. Линейные коды.
35. Циклические коды.
36. Групповые коды.
37. Матричные модели доступа.
38. Обыкновенные графы.
39. Ориентированные графы.
40. Графы с петлями и мультиграфы.
41. Нагруженные графы.
42. Коды Боуза-Чоудхури-Хоквингемы (БЧХ-коды).
43. Двоичные БЧХ-коды, исправляющие многократные ошибки.
44. Недвоичное кодирование.

4.2 Фонд оценочных средств для проведения промежуточной аттестации.

Список типовых алгоритмов (для самостоятельных и лабораторных занятий)

1. Найти период последовательности, заданной формулой .
2. Решить систему линейных уравнений по разным модулям
3. Привести пример регистра сдвига с обратной связью. Записать регистр в матричной форме. Нарисовать электронную схему регистра.
4. Привести пример кода, исправляющего 3 ошибки.
5. Найти расстояние Хэмминга между конкретными кодирующими словами.
6. Найти расстояние Хэмминга между конкретными множествами кодирующих слов.
7. Закодировать кодом Хэмминга данный набор объектов (например, слов в алфавите).
8. Привести пример линейного кода.
9. Привести пример циклического кода.
10. Привести пример кода являющего групповым и кода групповым не являющегося.
11. На примере системы с тремя ресурсами и тремя пользователями привести пример матрицы доступа.
12. Матрицы доступа, реализованные в операционных системах семейства Linux.
13. Привести пример графа частично упорядоченного множества.
14. Привести пример графа с петлями.
15. Привести пример мультиграфа.
16. Матричная запись нагруженного графа.
17. Пример конечной реляционной алгебры.
18. Примеры операций в реляционной алгебре.
19. Привести примеры коммерческих реляционных баз данных.
20. Перечислить признаки распределенных баз данных.

21. Привести примеры кодов Боуза-Чоудхури-Хоквингемы (БЧХ-коды).
22. Привести пример двоичного БЧХ-коды, исправляющего 7 ошибок.
23. Привести примеры недвоичное кодирования.

Примерные темы реферативных докладов

1. Линейные регистры сдвига с обратной связью (доклад на лабораторном занятии в виде презентации).
2. Коды Хэмминга и сжатие информации (отчет в письменной форме).
3. Реляционные алгебры (доклад на лабораторном занятии).
4. Коммерческие продукт, реализующие модель распределенных баз данных (отчет в письменной форме).
5. Решение квадратных уравнений в конечных полях с использованием логарифмов Якоби (доклад на лабораторном занятии в виде презентации).
6. Обзор популярных БЧХ-кодов (доклад на лабораторном занятии в виде презентации).
7. Недостатки модели Белла-Ла Падула (отчет в письменной форме).

Критерии оценивания результатов обучения

Критерии оценивания по зачету:

«зачтено»: студент владеет теоретическими знаниями по данному разделу, знает формы допускает незначительные ошибки; студент умеет правильно объяснять материал, иллюстрируя его примерами

«не зачтено»: материал не усвоен или усвоен частично, студент затрудняется привести примеры, довольно ограниченный объем знаний программного материала.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

5.1 Основная литература:

1. Рябко Б.Я, Фионов А.Н. Криптографические методы защиты информации, 2-е изд.

[Электронный ресурс]. – М.: Горячая линия-Телеком, 2017. - URL: https://e.lanbook.com/reader/book/111097
2. Глухов М.М., Круглов И.А., Пичкур А.Б., Черемушкин А.В. Введение в теоретико-числовые методы криптографии. [Электронный ресурс]. - СПб.: Лань, 2022. - https://reader.lanbook.com/book/210746

5.2 Дополнительная литература:

1. Бухштаб А.А. Теория чисел, 6-е изд. [Электронный ресурс]. - СПб.: Лань, 2022. - https://reader.lanbook.com/book/189329
2. Торстейнсон П., Ганеш Г.А. Криптография и безопасность в технологии .NET. 4-е изд. [Электронный ресурс]. – М.: Лаборатория знаний, 2020. – URL: https://e.lanbook.com/reader/book/151552

6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Пакет компьютерной алгебры Sage 8.3. Официальный сайт http://sagemath.org/
2. Пакет компьютерной алгебры Gap4r9p3. Официальный сайт http://www.gap-system.org/
3. Пакет компьютерной алгебры PARI/GP 2.11 Официальный сайт http://pari.math.u-bordeaux.fr/

7,2 Методические указания к самостоятельной подготовке студентов для выполнения практических заданий лабораторных занятий

Для выполнения домашнего практического задания необходимо разобрать материал по соответствующей теме лабораторного занятия. При этом используются указания, данные преподавателем в ходе занятия, а также теоретико-практический материал, имеющийся в источниках из списка основной литературы. Если студент не смог понять приведенный в указанных источниках разбор типовых примеров в той степени, чтобы самостоятельно использовать предложенный алгоритм для решения задания, то он может получить консультацию преподавателя.

7.3. Методические указания к самостоятельной подготовке студентов к выполнению контрольных работ

В течение семестра проводятся три контрольных работы, каждая из которых длится 45 минут и состоит из трех практических и одного теоретического задания. Тематика трех контрольных работ соответствует тематике трех содержательных разделов дисциплины: Каждое задание оценивается по пятибалльной шкале, высокая оценка ставится при получении не менее 16 баллов, нижний порог успешности составляет 7 баллов. Для подготовки к контрольной работе необходимо выполнять задания в ходе лабораторных занятий, а также домашние задания. В процессе самоподготовки студенту желательно ознакомиться с разбором опорных по рассматриваемым темам задач, имеющихся в пособиях из списка литературы. Выше в пункте 6.2 приведен список заданий, который включает в себя все типы практических заданий контрольных работ.

7.4. Методические рекомендации к самостоятельной подготовке студентов к реферативному докладу

Каждый студент должен подготовить в течение семестра реферативный доклад по одной из тем, предназначенной для самостоятельного изучения. Для подготовки доклада желательно кроме основных источников литературы использовать дополнительные источники, а также Интернет-ресурс. Доклад может быть представлен студентом на лабораторном занятии, возможно, в виде презентации, если тема занятия соответствует теме доклада. Также студент может представить отчет о подготовке реферативного доклада в письменной форме в конце семестра. Оформление письменного отчета должно удовлетворять требованиям: а) текст набирается 14 шрифтом на бумаге формата А 4; б) на титульном листе кроме

темы также указывается факультет, направление (бакалавриат), курс, группа, ФИО студента; в) содержание материала по объему составляет 4-5 страниц; г) список литературы содержит не менее двух источников (возможно, из списка литературы в пункте 7).

Примерные темы реферативных докладов

1. Алгебраическое и вероятностное определение шифр системы.
2. Криптосистемы с открытым ключом.
3. Понятие сертификата.
4. Криптосистема RSA. Выбор параметров.
5. Шифр AES
6. ГОСТ -89
7. Криптографические хэш-функции. Стандарты ГОСТ Р 34.11-2012 и SHA.
8. Схема Эль-Гамаля
9. Вычисления на эллиптической кривой.
10. Цифровая подпись. Схемы цифровой подписи.
11. Стандарты ГОСТ Р 34.
12. Стандарт DSS.
13. Анализ программного криптопродукта.

7.4. Методические указания к самостоятельной подготовке студентов к зачету

Согласно учебному плану дисциплины «Теоретико-числовые методы криптографии» итоговой формой контроля является зачет. Для допуска к зачету студент должен научиться на лабораторных занятиях решать практические задания по темам разделов 1-3 (табл. 4.1), выполнять домашние задания, а также успешно выполнить три контрольные работы. Типы практических заданий на зачет соответствуют заданиям из пункта 6.2. Также на зачете студентам предлагаются и теоретические задания, состоящие в письменном ответе на один из вопросов, приведенных в пункте 6.1. Количество практических и теоретических заданий зависит от активности и результативности работы студента в течение семестра. Если при условии хорошей посещаемости и активной работы на занятиях студент по трем контрольным работам и реферативному докладу заслужил высокие оценки, то он автоматически получает допуск к экзамену.

5.3. Интернет-ресурсы, в том числе современные профессиональные базы данных и информационные справочные системы

Электронно-библиотечные системы (ЭБС):

1. ЭБС «ЮРАЙТ» https://urait.ru/
2. ЭБС «УНИВЕРСИТЕТСКАЯ БИБЛИОТЕКА ОНЛАЙН» www.biblioclub.ru
3. ЭБС «BOOK.ru» https://www.book.ru
4. ЭБС «ZNANIUM.COM» www.znanium.com
5. ЭБС «ЛАНЬ» https://e.lanbook.com

Профессиональные базы данных:

1. Web of Science (WoS) http://webofscience.com/
2. Scopus http://www.scopus.com/
3. ScienceDirect www.sciencedirect.com
4. Журналы издательства Wiley https://onlinelibrary.wiley.com/
5. Научная электронная библиотека (НЭБ) http://www.elibrary.ru/
6. Полнотекстовые архивы ведущих западных научных журналов на Российской платформе научных журналов НЭИКОН http://archive.neicon.ru
7. Национальная электронная библиотека (доступ к Электронной библиотеке диссертаций Российской государственной библиотеки (РГБ) https://rusneb.ru/
8. Президентская библиотека им. Б.Н. Ельцина https://www.prlib.ru/
9. Электронная коллекция Оксфордского Российского Фонда

https://ebookcentral.proquest.com/lib/kubanstate/home.action

10. Springer Journals https://link.springer.com/
11. Nature Journals https://www.nature.com/siteindex/index.html
12. Springer Nature Protocols and Methods https://experiments.springernature.com/sources/springer-protocols
13. Springer Materials http://materials.springer.com/
14. zbMath https://zbmath.org/
15. Nano Database https://nano.nature.com/
16. Springer eBooks: https://link.springer.com/
17. "Лекториум ТВ" http://www.lektorium.tv/
18. Университетская информационная система РОССИЯ http://uisrussia.msu.ru

Информационные справочные системы:

1. Консультант Плюс - справочная правовая система (доступ по локальной сети с компьютеров библиотеки)

Ресурсы свободного доступа:

1. Американская патентная база данных http://www.uspto.gov/patft/
2. Полные тексты канадских диссертаций http://www.nlc-bnc.ca/thesescanada/
3. КиберЛенинка (http://cyberleninka.ru/);
4. Министерство науки и высшего образования Российской Федерации https://www.minobrnauki.gov.ru/;
5. Федеральный портал "Российское образование" http://www.edu.ru/;
6. Информационная система "Единое окно доступа к образовательным ресурсам" http://window.edu.ru/;
7. Единая коллекция цифровых образовательных ресурсов http://school-collection.edu.ru/ .
8. Федеральный центр информационно-образовательных ресурсов (http://fcior.edu.ru/);
9. Проект Государственного института русского языка имени А.С. Пушкина "Образование на русском" https://pushkininstitute.ru/;
10. Справочно-информационный портал "Русский язык" http://gramota.ru/;
11. Служба тематических толковых словарей http://www.glossary.ru/;
12. Словари и энциклопедии http://dic.academic.ru/;
13. Образовательный портал "Учеба" http://www.ucheba.com/;
14. Законопроект "Об образовании в Российской Федерации". Вопросы и ответы http://xn--273--84d1f.xn--p1ai/voprosy_i_otvety

Собственные электронные образовательные и информационные ресурсы КубГУ:

1. Среда модульного динамического обучения http://moodle.kubsu.ru
2. База учебных планов, учебно-методических комплексов, публикаций и конференций http://mschool.kubsu.ru/
3. Библиотека информационных ресурсов кафедры информационных образовательных технологий http://mschool.kubsu.ru;
4. Электронный архив документов КубГУ http://docspace.kubsu.ru/
5. Электронные образовательные ресурсы кафедры информационных систем и технологий в образовании КубГУ и научно-методического журнала "ШКОЛЬНЫЕ ГОДЫ" http://icdau.kubsu.ru/

6. Методические указания для обучающихся по освоению дисциплины (модуля).

Согласно учебному плану дисциплины «Информационная безопасность» итоговой формой контроля является зачет. Для сдачи зачета студент должен научиться на лабораторных занятиях решать практические задания по темам разделов 1-3, выполнять домашние задания. Типы практических заданий на зачет соответствуют заданиям. Также на

зачете студентам предлагаются и теоретические задания, состоящие в письменном ответе на один из вопросов. Количество практических и теоретических заданий зависит от активности и результативности работы студента в течение семестра.

Важнейшим этапом курса является самостоятельная работа по дисциплине (модулю).

Для подготовки к ответам на теоретические вопросы в ходе контрольных работ и на зачете студентам достаточно использовать материал лекций. Весь этот теоретический материал содержится в учебных пособиях из списка основной литературы. Для изучения теоретического материала, необходимого для подготовки реферативного доклада, кроме основных источников литературы возможно использование дополнительных источников и Интернет-ресурса. В случае затруднений, возникающих у студентов в процессе самостоятельного изучения теории, преподаватель разъясняет сложные моменты на консультациях.

7. Материально-техническое обеспечение по дисциплине (модулю)

По всем видам учебной деятельности в рамках дисциплины используются аудитории, кабинеты и лаборатории, оснащенные необходимым специализированным и лабораторным оборудованием.

При заполнении таблицы учитывать все виды занятий, предусмотренные учебным планом по данной дисциплине: лекции, занятия семинарского типа (практические занятия, лабораторные работы), а также курсовое проектирование, консультации, текущий контроль и промежуточную аттестацию.

При использовании лаборатории указать ее наименование «Лаборатория…».

Наименование специальных помещений	Оснащенность специальных помещений	Перечень лицензионного программного обеспечения
Учебные аудитории для проведения занятий лекционного типа	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер	
Учебные аудитории для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер Оборудование:	
Учебные аудитории для проведения лабораторных работ. Лаборатория…	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер Оборудование:	
Учебные аудитории для курсового проектирования (выполнения курсовых работ)	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер Оборудование:	

Для самостоятельной работы обучающихся предусмотрены помещения, укомплектованные специализированной мебелью, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Наименование помещений для самостоятельной работы обучающихся	Оснащенность помещений для самостоятельной работы обучающихся	Перечень лицензионного программного обеспечения
Помещение для самостоятельной работы обучающихся (читальный зал Научной библиотеки)	Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы	

	Оборудование: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, веб-камеры, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi)	
Помещение для самостоятельной работы обучающихся (ауд._____)	Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы Оборудование: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, веб-камеры, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi)	

№	Вид работ	Материально-техническое обеспечение дисциплины (модуля) и оснащенность
1.	Лекционные занятия	Лекционная аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) и соответствующим программным обеспечением (ПО) Программы, демонстрации видео материалов (проигрыватель «Windows Media Player»). Программы для демонстрации и создания презентаций («Microsoft Power Point»).
2.	Семинарские занятия	Не предусмотрены
3.	Лабораторные занятия	Лаборатория, укомплектованная специализированной мебелью и техническими средствами обучения – компьютерами с предустановленными GAP и Sage
4.	Курсовое проектирование	Не предусмотрено
5.	Групповые (индивидуальные) консультации	Аудитория для групповых занятий
6.	Текущий контроль, промежуточная аттестация	Аудитория для групповых занятий
7.	Самостоятельная работа	Кабинет для самостоятельной работы, оснащенный компьютерной техникой с возможностью подключения к сети «Интернет», программой экранного увеличения и обеспеченный доступом в электронную информационно-образовательную среду университета.