Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования «Северо-Осетинский государственный университет имени Коста Левановича Хетагурова»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Группы, кольца и теоретико-числовые основы в криптографии»

Направление подготовки 01.03.01 Математика

Профиль: "Алгебра, теория чисел, математическая логика"

Форма обучения – очная

Владикавказ, 2017

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 01.03.01 Математика, утвержденным приказом Министерства образования и науки Российской Федерации от 07.08.2014 г. № 943, учебным планом подготовки бакалавриата по направлению подготовки 01.03.01 Математика, профиль «Алгебра, теория чисел, математическая логика», утвержденным Ученым советом ФГБОУ ВО «СОГУ» от 27.04.2017 г. № 11.

Составитель: Дряева Р.Ю

Рабочая программа обсуждена и утверждена на заседании кафедры алгебры и геометрии (протокол № 8 от 28.03.2017 г.)

Одобрена советом факультета математики и информационных технологий (протокол № 5 от 31.03.2017 г.)

1. Структура и общая трудоемкость дисциплины

Общая трудоемкость дисциплины составляет 4 зачётные единицы.(144 час.).

	Очная Форма обучения
Курс	3
Семестр	5
Лекции	36
Практические занятия	54
Лабораторные занятия	-
Консультации	+
Итого аудиторных занятий	90
Самостоятельная работа	18
Курсовая работа	-
Зачет	-
Экзамен	36
Общее количество часов	144 час.

2. Цели освоения дисциплины

Целью освоения дисциплины "Группы, кольца и теоретико-числовые основы в криптографии" является формирование у студентов системы знаний в области криптографии, а также получение практических навыков в области криптографических методов защиты информации и криптоанализа. Дисциплина содержит основные положения криптографии, знакомит с наиболее распространенными типами шифров и методами их криптоанализа, понятиями целостности информации, криптографическими протоколами, электронной подписью. Объясняется математическая теория, лежащая в основе криптографии (теория групп, полей Галуа, неприводимые многочлены, теория чисел, псевдослучайные последовательности и др.). Ставятся вопросы реализации алгоритмов шифрования. В рамках лекционных занятий основное внимание уделяется изложению теоретических основ курса, доказательству основных теорем. Для закрепления теоретического материала на лекциях целесообразно проведение мини-опросов и коротких тестов. Главной задачей каждой лекции является раскрытие сущности темы и анализ ее главных положений. Содержание лекций определяется рабочей программой курса.

Целью практических занятий является закрепление теоретических знаний, выработка навыков решения задач.

3. Место дисциплины в структуре ОПОП:

Для изучения дисциплины необходимы знания, полученные обучающимися в рамках школьного курса «Информатика», а также в результате освоения дисциплин: «Компьютерные науки (Языки программирования)», «Компьютерные науки (Информатика)», «Алгебра», «Дискретная математика и математическая логика», «Математический анализ».

Приступая к изучению дисциплины «Группы, кольца и теоретико-числовые основы в криптографии», студент должен иметь представление об основных понятиях алгебры, комбинаторики, теории вероятности, информатики.

4. Требования к результатам освоения дисциплины

Компетенции обучающегося, формируемые в результате освоения дисциплины.

В результате изучения дисциплины обучающийся должен обладать следующими компетенциями (результатами освоения образовательной программы):

ОПК-1 -готовностью использовать фундаментальные знания в области математического анализа, комплексного и функционального анализа, алгебры, аналитической геометрии, дифференциальной геометрии и топологии, дифференциальных уравнений, дискретной математики и математической логики, теории вероятностей, математической статистики и случайных процессов, численных методов, теоретической механики в будущей профессиональной деятельности;

ОПК-3 -способностью к самостоятельной научно-исследовательской работе;

ПК-3 -способностью строго доказать утверждение, сформулировать результат, увидеть следствия полученного результата.

Взаимосвязь планируемых результатов обучения по дисциплине с формируемыми компетенциями ОПОП:

Компетенции		**Планируемые результаты обучения, соответствующие формируемым компетенциям ОПОП**		
Код	**Формулировка**	**Знать:**	**Уметь**	**Владеть:**
ОПК-1	готовностью использовать фундаментальные знания в области математического анализа, комплексного и функционального анализа, алгебры, аналитической геометрии, дифференциальной геометрии и топологии, дифференциальных уравнений, дискретной математики и математической логики, теории вероятностей, математической статистики и случайных процессов, численных методов, теоретической	основные понятия теории многочленов; перестановки; линейные пространства; линейные операторы и линейные отображения; теорию матриц; теории групп; методы и средства обеспечения информационной безопасности компьютерных систем; основные стандарты в области инфокоммуникационных систем и технологий; технологии обнаружения компьютерных атак и их возможности; основные уязвимости и типовые атаки на современные	применять полученные методы и модели к решению типовых и практических задач криптографии	навыки применения алгебраических методов для решения различных прикладных задач, связанных с распознаванием слов, в которых допущено некоторое количество ошибок

	механики в будущей профессиональной деятельности	компьютерные системы		
ОПК-3	способностью к самостоятельной научно-исследовательской работе	Основные научные подходы к исследуемому материалу	выделять и систематизировать основные идеи в научных текстах; критически оценивать любую поступающую информацию, вне зависимости от источника; избегать автоматического применения стандартных формул и приемов при решении задач.	навыками сбора, обработки, анализа и систематизации информации по теме исследования; навыками выбора методов и средств решения задач исследования
ПК-3	способностью строго доказать утверждение, сформулировать результат, увидеть следствия полученного результата	профессиональную терминологию, основные направления, проблемы, теории и методы теории групп и криптографии	использовать положения и теоремы математических наук для анализа и оценивания различных фактов и явлений в криптографических задачах	навыками анализа основных проблем, в т.ч. междисциплинарного характера

При проведении учебных занятий обеспечивается развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая при необходимости проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, преподавание дисциплин (модулей) в форме курсов, составленных на основе результатов научных исследований, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей).

5. Содержание и учебно-методическая карта дисциплины

Таблица 5.1

Номер недели	**Наименование тем (вопросов), изучаемых по данной дисциплине**	**Занятия**		**Самостоятельная работа студентов**		**Формы контроля**	**Баллы**		**Литература**
		л	пр	Содержание	Часы		min	max	
1	Группы. Примеры групп.	2	4	Построение конечных групп.	6	Устный опрос, сообщения по вопросам темы, конспект.	**0**	**10**	**[1-6]**
2	Фактор-группа. Примеры. Гомоморфизм групп. Теоремы о гомоморфизме.	2	2			Устный опрос, сообщения по вопросам темы, конспект.	**0**	**5**	**[1-6]**
3	Структура конечных циклических групп, конечные группы в криптографических системах.	2	4			Устный опрос, сообщения по вопросам темы, конспект.	**0**	**8**	**[1-6]**
4	Кольца. Примеры колец.	2	2	Построение конечных колец и полей. Построение неприводимых многочленов над полем из двух элементов.	6	Устный опрос, сообщения по вопросам темы, конспект.	**0**	**10**	**[1-6]**
5	Основные сведения о целых числах. Деление с остатком,	2	4			Устный опрос, сообщения по вопросам темы, конспект.	**0**	**6**	**[1-6]**

	алгоритм Евклида, множители Безу. Сравнение по модулю, кольца вычетов. Теоремы Эйлера и Ферма и обращение криптографического шифрования								
6	Китайская теорема об остатках. Криптосистемы с закрытым ключом. Простые подстановочные шифры. Шифр Хилла.	2	2			Устный опрос, сообщения по вопросам темы, конспект.	**0**	**4**	**[1-6]**
7	Принципы построения блочных шифров с закрытым ключом.	2	4			Устный опрос, сообщения по вопросам темы, конспект.	**0**	**4**	**[1-6]**
8-9	Алгоритмы шифрования DES и AES.	2	6	Исследование связи между алгоритмами DES и AES, ГОСТ 28147-89	6	Устный опрос, сообщения по вопросам темы, конспект.	**0**	**10**	**[1-6]**
10	Алгоритм криптографического преобразования ГОСТ 28147-89.	2	2		2	Устный опрос, сообщения по вопросам темы, конспект.	**0**	**4**	**[1-6]**
11	Криптографические хеш-функции.	2	4			Устный опрос, сообщения по вопросам	**0**	**4**	**[1-6]**

						темы, конспект.			
12-13	Поточные шифры и генераторы псевдослучайных чисел.	2	6			Устный опрос, сообщения по вопросам темы, конспект.	**0**	**10**	**[1-6]**
14-15	Криптосистемы с открытым ключом. Основные положения теории чисел, используемые в криптографии с открытым ключом. Элементы теории алгоритмов. Криптографическая система RSA. Вопросы практического использования алгоритма RSA.	2	6			Устный опрос, сообщения по вопросам темы, конспект.	**0**	**10**	**[1-6]**
16	Электронная цифровая подпись.	2	2			Устный опрос, сообщения по вопросам темы, конспект.	**0**	**5**	**[1-6]**
17	Совершенно секретные системы.	2	4			Устный опрос, сообщения по вопросам темы, конспект.	**0**	**4**	**[1-6]**
18	Шифрование, помехоустойчивое кодирование и сжатие информации	2	2			Устный опрос, сообщения по вопросам	**0**	**6**	**[1-6]**

						темы, конспект.			
	ИТОГО	36	54		18		**0**	**100**	

Примечания:

– Все виды учебной работы могут проводиться дистанционно на основании локальных нормативных актов.

– В целях реализации индивидуального подхода к обучению студентов, осуществляющих учебный процесс по индивидуальной траектории в рамках индивидуального рабочего плана, изучение данной дисциплины может осуществляться через индивидуальные консультации преподавателя очно, в часы консультаций, по электронной почте и с использованием платформ дистанционного обучения.

6. Образовательные технологии

В соответствии с государственными образовательными стандартами высшего образования реализация учебного процесса должна предусматривать проведение занятий в интерактивных и активных формах. Внедрение этих форм обучения – одно из важнейших направлений совершенствования подготовки студентов в современном вузе. Цель – повышение эффективности образовательного процесса, достижение всеми обучающимися высоких результатов обучения.

Интерактивные формы проведения занятий предполагают обучение в сотрудничестве. Все участники образовательного процесса (преподаватель и студенты) взаимодействуют друг с другом, обмениваются информацией, совместно решают проблемы, моделируют ситуации. Суть использования активных и интерактивных форм проведения состоит в погружении студентов в реальную атмосферу делового сотрудничества по разрешению проблем, оптимальную для выработки навыков и качеств будущего специалиста.

Для решения воспитательных и учебных задач преподавателем могут быть использованы следующие интерактивные формы обучения.

Традиционные лекции и практические (семинарские) занятия с использованием современных интерактивных технологий.

Лекция-диалог – содержание подается через серию вопросов, на которые студент должен отвечать непосредственно в ходе лекции.

Онлайн-семинар – разновидность веб-конференции, проведение онлайн-встреч или презентаций через Интернет в режиме реального времени. Каждый из участников находится у своего компьютера (средства связи), а связь между ними поддерживается через Интернет посредством загружаемого приложения, установленного на компьютере каждого участника.

Видеоконференция – сеанс видеоконференцсвязи (ВКС) – это технология интерактивного взаимодействия двух и более участников образовательного процесса для обмена информацией в реальном режиме времени.

Видео-лекция – снятая на камеру сокращенная лекция, дополненная фотографиями и схемами, иллюстрирующая подаваемый в лекции материал.

Технология электронного обучения (реализуется при помощи электронной образовательной среды СОГУ при использовании ресурсов ЭБС, при проведении автоматизированного тестирования и т. д.).

Творческое заданиесоставляет содержание (основу) любой интерактивной формы проведения занятия. Выполнение творческих заданий требует от студента воспроизведения полученной ранее информации в форме, определяемой преподавателем и требующей творческого подхода: 1) подборка примеров из практики; 2) подборка материала по определенной проблеме;

Публичная презентация проекта - самый эффективный способ донесения важной информации при публичных выступлениях. Слайд-презентации позволяют эффектно и наглядно представить содержание, выделить и проиллюстрировать сообщение.

Интерактивная лекция представляет собой выступление преподавателя перед аудиторий студентов с применением следующих интерактивных форм обучения: 1. управляемая дискуссия или беседа; 2. демонстрация слайдов или учебных фильмов; 3. мозговой штурм; 4. мотивационная речь и др.

Разработка проекта позволяет участникам мысленно выйти за пределы аудитории и составить проект своих действий по обсуждаемому вопросу Участники могут обратиться за консультацией, дополнительной литературой в специализированные учреждения, библиотеки и т.д.

Проблемное обучение- поиск ответов на вопросы по теме.

7. Учебно-методическое обеспечение самостоятельной работы

Самостоятельная работа обучающихся является одним из видов учебных занятий. Самостоятельная работа проводится с целью:

− систематизации и закрепления полученных теоретических знаний и практических умений обучающихся студентов;

− углубления и расширения теоретических знаний;

− формирования умений использовать нормативную, правовую, справочную документацию и специальную литературу;

- формирования самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;

− развития исследовательских умений.

К видам самостоятельной работы при изучении данной дисциплины относится: написание докладов, эссе, подготовка презентаций, самостоятельное изучение литературы по теме и составление по ней конспектов, работа со справочными материалами (терминологическими и иными словарями, энциклопедиями) и т.д.

Темы и формы внеаудиторной самостоятельной работы, ее трудоёмкость содержатся в разделе 5, табл. 5.1.

Методические рекомендации по дисциплине прилагаются.

8. Оценочные средства для текущего контроля успеваемости, рубежной аттестации и промежуточной аттестации по итогам освоения дисциплины

Рабочая программа предусматривает проведение лекционных и практическихзанятий, а также следующие виды работ: самостоятельную работу студентов по подготовке устных сообщений, написанию докладов, подготовку презентаций и обсуждений по темам дисциплины - работу в активной и интерактивной формах.

Рабочая программа предполагает текущий и промежуточный контроль знаний.

Текущий контроль – это непрерывно осуществляемый мониторинг уровня усвоения знаний и формирования умений и навыков в течение семестра или учебного года. Текущий контроль знаний, умений и навыков студентов осуществляется в ходе учебных (аудиторных) занятий, проводимых по расписанию. Формами текущего контроля выступают опросы на занятияхс целью проверки наличия знаний, необходимых для усвоения нового материала или для выяснения степени усвоения изложенного материала.

Рубежный контроль осуществляется по окончании изучения материала модуля в заранее установленное время. Рубежный контроль проводится с целью определения качества усвоения материала учебного модуля в целом. В течение семестра такие контрольные мероприятия проводятся по графику.

Контрольные задания (демоверсии) для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

1. Проверить какие из отображений являются гомоморфизмами групп:

a) $f: R \to R^*$, где $f(x) = e^x$;

b) $f: M_n(R) \to R^*$, где $f(A) = a_{11}$.

   Найти ядро и образ гомоморфизма.

2. В криптосистеме RSA p=5, q=11. Вычислите открытый и закрытый ключи и зашифруйте сообщение m=7.
3. Найдите число x<385, если

$$\begin{cases} x\ mod\ 5 = 1 \\ x\ mod\ 7 = 4 \\ x\ mod\ 11 = 10 \end{cases}$$

4. В криптосистеме Хилла с инволютивной над Z_{26} матрицей $\begin{pmatrix} 2 & 7 \\ 7 & 24 \end{pmatrix}$ зашифруйте слово CRYPTOGRAPHY
5. Первый байт фрагмента текста имеет вид C7,на него накладывается по модулю 2 4-х битовая гамма 0111. Что получится после шифрования?

Критерии оценивания представлены в таблице 8.1.

Примеры тестовых заданий по дисциплине:

1. Найти порядки всех элементов в $Z_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$
   +$|\bar{1}| = 6, |\bar{2}| = 3, |\bar{3}| = 2, |\bar{4}| = 3, |\bar{5}| = 6$
   -$|\bar{1}| = 6, |\bar{2}| = 3, |\bar{3}| = 2, |\bar{4}| = 6, |\bar{5}| = 12$
   -$|\bar{1}| = 6, |\bar{2}| = 3, |\bar{3}| = 4, |\bar{4}| = 3, |\bar{5}| = 6$
2. Какое количество образующих в группе $G = Z_{20}$?
   +8
   2
   12
3. Используя теорему Эйлера и алгоритм быстрого возведения в степень, найти $32^{102}(mod\ 45)$
   +9
   0
   1
4. Зашифровать сообщение « Признак хорошего образования — говорить о самых высоких предметах самыми простыми словами» с помощью таблицы Вижинера и ключа «*Эмерсон*»
   +мэншяоштыхяйурлыёбсцьямтщр — сьяыхщдк ь
   омслжриоыпщжююврсхдогомслючэныцгмыцошутсыц
   мэншяоштыхяйурлыёбсцьямтщр — бьяыхщдк ь
   омнлжриоыпщжююврсхдогомслючэныцгмыцошутсыц
   мэншяоштыхяйурлыёбсцьямтщр — сьяыхщдк ь
   омслжсиоыпщжяюврсхдогомслючэныцгмыцошутсыц
5. Произвести вычисление псевдослучайной последовательности по алгоритму RC4 (n=3) и найти z_1, z_2, z_3. Секретный ключ: 2,3,1,4.
   +$z_1 = 3, z_2 = 1, z_3 = 5$
   -$z_1 = 3, z_2 = 1, z_3 = -5$
   -$z_1 = 3, z_2 = 2, z_3 = 4$

Методика формирования результирующей оценки

Таблица 8.1

Этап	**Форма контроля**	**Критерии оценивания (процент от максимального кол-ва баллов)**			
		86-100 %	**71–85%**	**60–70%**	**Менее 60%**
1. Текущий контроль (max 25 баллов за 1 модуль)					
		7-8 баллов	6–7 баллов	4–5 баллов	0–3 баллов
	Посещени	Студент	Студент	Студент	Студент посетил

	е занятий (max 8 б.)	посетил более 85% занятий	посетил 71–85% занятий	посетил 56–70% занятий	менее 56% занятий
		9–10 баллов	7–8 баллов	6–7 баллов	0–5 баллов
	Текущая работа в течение модуля (max 10б.)	Студент активно работает на занятиях, превосходно выполняет все задания преподавателя.	Студент активно работает на занятиях, хорошо выполняет задания преподавателя.	Студент недостаточно активно работает на занятиях, удовлетворительно выполняет задания преподавателя.	Студент недостаточно активно работает на занятиях, неудовлетворительно выполняет задания преподавателя.
		3/2 балла	2 балла	1 балл	0 баллов
	Доклад, презентация (max 3б.) / опорный конспект (max 2б.)	Тема полностью раскрыта. Превосходное владение материалом. Высокий уровень самостоятельности, логичности, аргументированности. Превосходный стиль изложения.	Тема в основном раскрыта. Хорошее владение материалом. Средний уровень самостоятельности, логичности, аргументированности. Хороший стиль изложения.	Тема частично раскрыта. Удовлетворительное владение материалом. Низкий уровень самостоятельности, логичности, аргументированности. Удовлетворительный стиль изложения.	Тема не раскрыта. Неудовлетворительное владение материалом. Недостаточный уровень самостоятельности, логичности, аргументированности. Неудовлетворительный стиль изложения.
2. Рубежный контроль (25б. за 1 модуль)					
		22–25 баллов	18–21 балл	14–17 баллов	0–13 баллов
	Контрольная работа	Правильно выполнены все задания. Продемонстрирован высокий уровень владения материалом. Проявлены превосходные способности применять знания и умения к выполнению конкретных заданий.	Правильно выполнена большая часть заданий. Присутствуют незначительные ошибки. Продемонстрирован хороший уровень владения материалом. Проявлены средние способности применять знания и умения к выполнению конкретных заданий.	Задания выполнены более чем наполовину. Присутствуют серьезные ошибки. Продемонстрирован удовлетворительный уровень владения материалом. Проявлены низкие способности применять знания и умения к выполнению конкретных	Задания выполнены менее чем наполовину. Продемонстрирован неудовлетворительный уровень владения материалом. Проявлены недостаточные способности применять знания и умения к выполнению конкретных заданий.

				заданий.	
3. Итоговый контроль по дисциплине					
		43–50 баллов	36–42 балла	28–35 баллов	0–27 баллов
	Экзамен/зачет	Дан полный, развернутый ответ на поставленный вопрос. Ответ формулируется в терминах науки, изложен литературным языком, логичен, доказателен, демонстрирует авторскую позицию студента.	Дан полный ответ на поставленный вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи. Но допущены незначительные ошибки, исправленные студентом с помощью «наводящих» вопросов преподавателя.	Дан недостаточно полный ответ. Студент не способен самостоятельно выделить существенные и несущественные признаки и причинно-следственные связи. Речевое оформление требует поправок, коррекции.	Не получены ответы по базовым вопросам дисциплины или дан неполный ответ и допущены грубые ошибки. Речь неграмотная. Уточняющие вопросы преподавателя не приводят к коррекции ответа студента не только на поставленный вопрос, но и на другие вопросы дисциплины.

Студенты, получившие в ходе текущего и рубежного контроля 56-100 баллов, автоматически получают «Зачет» или соответствующую шкале экзаменационную оценку. Результирующая оценка складывается по соответствующей БРС формуле.

Вопросы для подготовки к экзамену:

1. Группы. Примеры групп.
2. Подгруппы. Примеры подгрупп.
3. Циклические группы.
4. Гомоморфизм и изоморфизм групп.
5. Классы смежности. Фактор-группа.
6. Теоремы о гомоморфизме.
7. Действие группы на множестве. Стабилизатор.
8. Кольца. Поля. Примеры.
9. Кольцо классов вычетов. Нильпотенты и делители нуля.
10. Конечные поля.
11. Расширения полей.
12. Делимость целых чисел
13. Простые числа. Бесконечность числа простых чисел
14. НОД целых чисел. Алгоритм Евклида. Функция Эйлера

15. Решение систем сравнений. Китайская теорема об остатках.
16. Шифр Цезаря, Вижинера. Методы перестановки, гаммирования.
17. Криптосистемы с закрытым ключом. Простые подстановочные шифры. Шифр Хилла.
18. Криптосистемы с открытым ключом. Криптографическая система RSA.
19. Совершенно секретные системы. Генераторы псевдослучайных чисел.
20. Хеш-функции.
21. Электронная подпись.
22. Криптосистема электронной подписи по протоколу RSA.

Показатели и критерии оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Уровень сформированности компетенций			
«Минимальный уровень не достигнут» (менее 56 баллов)	**«Минимальный уровень» (56-70 баллов)**	**«Средний уровень» (71-85 баллов)**	**«Высокий уровень» (86-100 баллов)**
Компетенции не сформированы. Знания отсутствуют, умения и навыки не сформированы.	*Компетенции сформированы.* Сформированы базовые структуры знаний. Умения фрагментарны и носят репродуктивный характер. Демонстрируется низкий уровень самостоятельности практического навыка.	*Компетенции сформированы.* Знания обширные, системные. Умения носят репродуктивный характер, применяются к решению типовых заданий. Демонстрируется достаточный уровень самостоятельности устойчивого практического навыка.	*Компетенции сформированы.* Знания твердые, аргументированные, всесторонние. Умения успешно применяются к решению как типовых, так и нестандартных творческих заданий. Демонстрируется высокий уровень самостоятельности, высокая адаптивность практического навыка
Описание критериев оценивания			
Обучающийся демонстрирует: - существенные пробелы в знаниях учебного материала; - допускаются принципиальные ошибки при ответе	Обучающийся демонстрирует: - знания теоретического материала; - неполные ответы на основные вопросы, ошибки в	Обучающийся демонстрирует: - знание и понимание основных вопросов контролируемого объема программного	Обучающийся демонстрирует: - глубокие, всесторонние и аргументированные знания программного материала;

на основные вопросы, отсутствует знание и понимание основных понятий и категорий; -непонимание сущности дополнительных вопросов в рамках заданий; - отсутствие умения выполнять практические задания, предусмотренные программой дисциплины; - отсутствие готовности (способности) к дискуссии и низкую степень контактности.	ответе, недостаточное понимание сущности излагаемых вопросов; - неуверенные и неточные ответы на дополнительные вопросы; - недостаточное владение литературой, рекомендованной программой дисциплины; - умение без грубых ошибок решать практические задания, которые следует выполнить.	материала; - твердые знания теоретического материала. -способность устанавливать и объяснять связь практики и теории, выявлять противоречия, проблемы и тенденции развития; - правильные и конкретные, без грубых ошибок, ответы на поставленные вопросы; - умение решать практические задания, которые следует выполнить; - владение основной литературой, рекомендованной программой дисциплины; - наличие собственной обоснованной позиции по обсуждаемым вопросам. Возможны незначительные оговорки и неточности в раскрытии отдельных положений вопросов, присутствует неуверенность в ответах.	- полное понимание сущности и взаимосвязи рассматриваемых процессов и явлений, точное знание основных понятий в рамках обсуждаемых заданий; - способность устанавливать и объяснять связь практики и теории; - логически последовательные, содержательные, конкретные и исчерпывающие ответы на все задания, а также дополнительные вопросы экзаменатора; - умение решать практические задания; - свободное использование в ответах на вопросы материалов рекомендованной основной и дополнительной литературы.
Оценка «неудовлетворительно» /не зачтено	**Оценка «удовлетворительно» / «зачтено»**	**Оценка «хорошо» / «зачтено»**	**Оценка «отлично» / «зачтено»**

9. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1. Ельчанинова, Н.Б. Правовые основы защиты информации с ограниченным доступом : учебное пособие / Н.Б. Ельчанинова ; Министерство науки и высшего образования РФ, Южный федеральный университет, Инженерно-технологическая академия. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2017. – 77 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=499598
2. Лапонина, О.Р. Межсетевые экраны : учебное пособие / О.Р. Лапонина. – 2-е изд., исправ. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 466 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=429093 .
3. Мэйволд, Э. Безопасность сетей / Э. Мэйволд. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 572 с. : схем., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=429035
4. Технологии защиты информации в компьютерных сетях / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суровов. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 369 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=428820

б) дополнительная литература:

5. Голиков, А.М. Защита информации от утечки по техническим каналам : учебное пособие : [16+] / А.М. Голиков ; Томский Государственный университет систем управления и радиоэлектроники (ТУСУР). – Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. – 256 с. : схем., табл., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=480636
6. Пилиди, В.С. Математические основы защиты информации : учебное пособие : [16+] / В.С. Пилиди ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2019. – 309 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=577894

в) электронные библиотечные системы, с которыми у СОГУ имеется действующий договор, современные профессиональные базы, информационные справочные системы:

– eLIBRARY.RU [Электронный ресурс]: научная электронная библиотека. – URL: http://www.elibrary.ru.

– База данных «ЭБС elibrary»: http://elibrary.ru

– Издательство «Юрайт» [Электронный ресурс]: электронно-библиотечная система. – URL: http://biblio-online.ru.

- Университетская библиотека online [Электронный ресурс]: электронно-библиотечная система. – URL: http://www.biblioclub.ru.

10. Материально-техническое обеспечение дисциплины

Занятия по дисциплине проводятся в аудиториях, обеспеченных компьютерами, имеющими доступ к сети Интернет, интерактивными досками и мультимедийным оборудованием.

Лицензионное программное обеспечение:

1. Windows 10 Pro for Workstations, (№ 4100072800 Microsoft Products (MPSA) от 04.2016г);
2. Office Standard 2016 (№ 4100072800 Microsoft Products (MPSA) от 04.2016г);
3. Система поиска текстовыхзаимствований «Антиплагиат ВУЗ»;

Перечень ПО в свободном доступе:

1. Kaspersky Free;
2. WinRar;
3. Google Chrome;
4. Yandex Browser;
5. OperaBrowser;

11. Лист обновления/актуализации

1. Рабочая программа

пересмотрена и актуализирована на заседании кафедры алгебры и геометрии протокол № 8 от 22.03 2018г.;

одобрена на заседании совета факультета математики и информационных технологий. протокол № 5 от 30.03.2018)

2. Рабочая программа

пересмотрена и актуализирована на заседании кафедры алгебры и геометрии протокол № 7 от 27.03.2019г.;

одобрена на заседании совета факультета математики и информационных технологий, протокол № 5 от 29.03.2019 г.

3. Рабочая программа

пересмотрена и актуализирована на заседании кафедры алгебры и геометрии; протокол №7 от24.03.2020)

одобрена на заседании совета факультета математики и информационных технологий, протокол № 5 от 27.03.2020 г.