

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



**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Криптография в задачах»**

Направление подготовки 09.03.01 Информатика и вычислительная техника

Профиль: Информатика и вычислительная техника

Форма обучения – очная

Владикавказ, 2017

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 09.03.01 Информатика и вычислительная техника Профиль Информатика и вычислительная техника, утвержденным приказом Министерства образования и науки Российской Федерации от 12.01.2016 г. № 5, учебным планом подготовки бакалавриата по направлению подготовки 09.03.01 Информатика и вычислительная техника Профиль Информатика и вычислительная техника, 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» марта 2017 г.

одобрена советом факультета математики и информационных технологий
(протокол № 5 от «31» марта 2017 г.)

1. Структура и общая трудоемкость дисциплины

Общая трудоемкость дисциплины составляет 2 зачётные единицы. (72 час.).

	Очная Форма обучения
Курс	3
Семестр	6
Лекции	16
Практические занятия	34
Лабораторные занятия	-
Консультации	-
Итого аудиторных занятий	50
Самостоятельная работа	22
Курсовая работа	-
Зачет	-
Экзамен	-
Общее количество часов	72 час.

2. Цели освоения дисциплины

Целями освоения дисциплины (модуля) «Криптография в задачах» является изучение классических методов криптографической защиты информации и современных методов обеспечения конфиденциальности и целостности данных, ориентированных на применение вычислительной техники. В рамках курса рассматриваются практические аспекты информационной безопасности автоматизированных систем.

Практические работы в компьютерных классах служат для индивидуальной работы студентов над учебными задачами с целью выработки и закрепления практических навыков курса.

3. Место дисциплины в структуре ОПОП:

Дисциплина «Криптография в задачах» относится к дисциплинам Блок 1. Дисциплины (модули). Вариативная часть. Дисциплины по выбору. Б1.В.ДВ.14.01.

Для изучения дисциплины необходимы знания, полученные обучающимися в рамках школьного курса «Информатика», а также в результате освоения дисциплин: «Информатика», «Алгебра и геометрия», «Математический анализ».

Приступая к изучению дисциплины «Криптография в задачах», студент должен иметь представление об основных понятиях алгебры, комбинаторики, информатики, теориях чисел, сложности, вероятности.

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-5 -способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

ПК-1 -способностью разрабатывать модели компонентов информационных систем, включая модели баз данных и модели интерфейсов "человек - электронно-вычислительная машина".

Взаимосвязь планируемых результатов обучения по дисциплине с формируемыми компетенциями ОПОП:

Компетенции		Планируемые результаты обучения, соответствующие формируемым компетенциям ОПОП		
Код	Формулировка	Знать:	Уметь	Владеть:
ОПК-5	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	требования к обеспечению информационной безопасности	формулировать задачи защиты информации; использовать современные инструментальные средства защиты информации; уметь оценивать стойкость систем;	решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий с учетом основных требований информационной безопасности
ПК-1	способностью разрабатывать модели компонентов информационных систем, включая модели баз данных и модели интерфейсов "человек - электронно-вычислительная машина"	теоретические основы защиты компьютерной информации, криптографии; принципы построения систем защиты информации и их программной реализации	формировать схему защиты компьютерной информации; разрабатывать программы на основе изучаемых алгоритмов криптографии; разрабатывать модели компонентов информационных систем, включая модели баз данных;	разработки и реализации программного обеспечения защиты информации, криптографических систем и комплексов;

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		мин	сек	
1	Основные протоколы: разделение секрета, привязка к биту, подбрасывание монетки.	2	2	Электронная ставка. Схема Блэкли	2	Конспект, вопросы на коллоквиуме	0	10	[1-5]
2-3	Византийское соглашение, покер по телефону.	2	2	Протокол для $n \geq 3m+1$	2	Конспект, вопросы на коллоквиуме	0	10	[1-5]
4-5	Электронные выборы.	2	4	FOO-схема	2	Конспект, вопросы на коллоквиуме	0	10	[1-5]
6-7	Электронные деньги.	2	4	Слепая подпись	2	Конспект, вопросы на коллоквиуме	0	10	[1-5]
8-9	Введение в нулевое разглашение.	2	2	$IP \subseteq PSPACE$	2	Конспект, вопросы на коллоквиуме	0	10	[1-5]
10-11	Нулевое разглашение для класса NP.	2	4	Стойкость протокола	2	Конспект, вопросы на коллоквиуме	0	10	[1-5]
12-13	Забывчивая передача данных, проверяемое разделение секрета.		4	Модель Рабина	2	Конспект, вопросы на коллоквиуме	0	10	[1-5]
14-15	Многосторонние секретные вычисления.	2	4	Нечестные участники	2	Конспект, вопросы на коллоквиуме	0	10	[1-5]
16-17	Псевдослучайные генераторы.	2	4	Криптосистема на основе генератора	4	Конспект, вопросы на коллоквиуме	0	10	[1-5]
18	Псевдослучайные функции.		4	Задачи	2	Конспект, вопросы на коллоквиуме	0	10	[1-5]
	ИТОГО	16	34		22		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 задание составляет 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 аудиторией 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.

№/ п	Тема	Вид занятия	Количество часов	Активные формы	Интерактивные формы
1	Односторонние функции. Однонаправленные хэш-функции.	Практическое	4	Диалог	Интерактивная лекция
2	Прикладные программные интерфейсы, реализующие средства защиты информации	Практическое	4	Презентация	Интерактивная лекция
3	Защищенные транспортные протоколы. Программно-аппаратные средства защиты информации	Практическое	4	Доклад	Интерактивная лекция
	Итого		12		

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 относятся: 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 практических занятий, 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 занятиях с 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. Недостатки схемы Шаума
2. Доказать, что для любого $n \neq 2$ существует циклическая последовательность периода n , которой соответствует неприводимый в $GF(2)$ полином степени n . Построить криптограмму заданного сообщения, используя указанные циклические последовательности.

Критерии оценивания представлены в таблице 8.1.

Примеры тестовых заданий по дисциплине:

1) Модель Харисона-Руззо-Ульмана предназначена для анализа систем защиты, реализующих:

- дискреционную политику безопасности
- ролевую политику безопасности
- мандатную политику безопасности
- гибридную политику безопасности

2) Укажите основной недостаток модели Харисона-Руззо-Ульмана.

- Простота реализации
- Незащищенность перед «троянскими» программами
- Сложность реализации
- Сложность управления полномочиями пользователей

3) Укажите основной недостаток модели Белла-ЛаПадулы.

- Простота реализации
- Незащищенность перед «троянскими» программами
- Сложность реализации
- Сложность управления полномочиями пользователей

4) В модели Белла-ЛаПадулы состояние называется безопасным по чтению, когда:

- для каждого субъекта, осуществляющего в этом состоянии доступ чтения к объекту, уровень безопасности этого субъекта доминирует над уровнем безопасности этого объекта;
- для каждого субъекта, осуществляющего в этом состоянии доступ записи к объекту, уровень безопасности этого объекта доминирует над уровнем безопасности этого субъекта;

- когда оно безопасно и по чтению, и по записи;
 - такого понятия не существует.
- 5) В модели Белла-ЛаПадулы состояние называется безопасным по записи, когда:**
- для каждого субъекта, осуществляющего в этом состоянии доступ чтения к объекту, уровень безопасности этого субъекта доминирует над уровнем безопасности этого объекта;
 - для каждого субъекта, осуществляющего в этом состоянии доступ записи к объекту, уровень безопасности этого объекта доминирует над уровнем безопасности этого субъекта;
 - когда оно безопасно и по чтению, и по записи;
 - такого понятия не существует.
- 6) Система $\Sigma(v_0, Q, FT)$ безопасна тогда и только тогда, когда ее начальное состояние v_0 безопасно и все состояния, достижимые из v_0 путем применения конечной последовательности запросов из Q , безопасны. Это -**
- Критерий безопасности модели Харисона-Руззо-Ульмана
 - Критерий безопасности модели Белла-ЛаПадулы
 - Универсальный критерий для всех моделей разграничения прав
 - Критерий безопасности модели ролевого разграничения доступа
- 7) Роль – это:**
- Совокупность прав доступа на объекты компьютерной системы
 - Совокупность записей о событиях, связанных с работой системы безопасности
 - Право субъекта получать беспрепятственный доступ к объекту компьютерной системы
 - Право доступа субъекта к конфиденциальной информации.
- 8) Система функционирует безопасно тогда и только тогда, когда пользователь U , работающий в сессии s , может осуществлять действия в рамках права доступа r при условии, что $r \in \text{Permission}(s)$. Это:**
- Критерий безопасности модели Харисона-Руззо-Ульмана
 - Критерий безопасности модели Белла-ЛаПадулы
 - Универсальный критерий для всех моделей разграничения прав
 - Критерий безопасности модели ролевого разграничения доступа
- 9) Какого типа политики безопасности не существует:**
- Дискреционной политики безопасности
 - ролевой политики безопасности
 - мандатной политики безопасности
 - полимандатной политики безопасности
- 10) Критерий безопасности модели Белла-ЛаПадулы оценивает безопасность систем защиты, реализующих:**
- дискреционную политику безопасности
 - ролевую политику безопасности
 - мандатную политику безопасности
 - гибридную политику безопасности
- 11) Риск – это ситуация, когда:**
- угроза использует уязвимое место для нанесения вреда вашей системе
 - возникают неполадки в аппаратной части компьютерной системы
 - возникают неполадки в программной части компьютерной системы
- 12) Идентификатор SID :**
- служит основой для идентификации субъектов внутренними процессами ОС Windows;

- содержит идентификаторы безопасности, связанные с пользователем и его привилегии;
- служит для хранения данных о правах доступа к объекту доступа;
- хранит записи о событиях, связанных с работой системы безопасности

13) Дескриптор защиты

- служит основой для идентификации субъектов внутренними процессами ОС Windows;
- содержит идентификаторы безопасности, связанные с пользователем и его привилегии;
- служит для хранения данных о правах доступа к объекту доступа;
- хранит записи о событиях, связанных с работой системы безопасности

14) Система контроля учетных записей пользователя Windows Vista, Windows 7 называется:

- UAC
- SAM
- SID
- DACL

15) Хранит записи о событиях, связанных с работой системы безопасности

- Маркер доступа
- Дескриптор защиты
- Журнал аудита:
- Идентификатор SID

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
	Посещение занятий (max 8 б.)	Студент посетил более 85% занятий	Студент посетил 71–85% занятий	Студент посетил 56–70% занятий	Студент посетил 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	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.	Тема не раскрыта. Неудовлетворительное владение материалом. Недостаточный уровень самостоятельности, логичности, аргументированности.

		стиль изложения.		Удовлетворительный стиль изложения.	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. Продemonстрирован высокий уровень владения материалом. Проявлены превосходные способности применять знания и умения к выполнению конкретных заданий.	Правильно выполнена большая часть заданий. Присутствуют незначительные ошибки. Продemonстрирован хороший уровень владения материалом. Проявлены средние способности применять знания и умения к выполнению конкретных заданий.	Задания выполнены более чем наполовину. Присутствуют серьезные ошибки. Продemonстрирован удовлетворительный уровень владения материалом. Проявлены низкие способности применять знания и умения к выполнению конкретных заданий.	Задания выполнены менее чем наполовину. Продemonстрирован неудовлетворительный уровень владения материалом. Проявлены недостаточные способности применять знания и умения к выполнению конкретных 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 зачету:

1. Информационная безопасность.
2. Сущность и содержание защиты информации.
3. Цели и задачи защиты информации.
4. Основные определения теории защиты информации.
5. Источники атак на информацию.
6. Риски атак на информацию.
7. Формы атак на информацию.

8. Нормативные документы в области защиты информации.
9. Безопасность АСОИ.
10. Понятие санкционированного и несанкционированного доступов.
11. Базовые свойства безопасности информации.
12. Угрозы безопасности и каналы реализации угроз.
13. Основные принципы обеспечения информационной безопасности в АСОИ.
14. Меры обеспечения безопасности компьютерных систем.
15. Политика безопасности. Классификация политик безопасности.
16. Политики избирательного разграничения доступа.
17. Мандатные политики безопасности.
18. Контроль доступа, базирующийся на ролях.
19. Политики безопасности контроля целостности информационных ресурсов.
20. Классификация подсистем идентификации и аутентификации субъектов.
21. Парольные системы идентификации и аутентификации пользователей.
22. Идентификация и аутентификация пользователей с использованием технических устройств.
23. Идентификация и аутентификация с использованием индивидуальных биометрических характеристик пользователя.
24. Классы сложности алгоритмов.
25. Делимость и алгоритм Евклида.
26. Разложение числа на множители.
27. Квадратичные вычеты.
28. Закон взаимности и китайская теорема об остатках.
29. Простота и факторизация.
30. Стойкость криптосистем.
31. Гипотеза $P \neq NP$.
32. Односторонние функции.
33. Однонаправленные хэш-функции.
34. Модулярная арифметика.
35. Простые числа и их свойства.
36. Числовые функции.
37. Принципы криптографической защиты информации.
38. Ключи шифрования.
39. Традиционные симметричные криптосистемы
40. Шифрование методом замены.
41. Шифрование методами перестановки.
42. Шифрование методом гаммирования
43. Шифрование методом Цезаря.
44. Простая моноалфавитная замена.
45. Шифрующие таблицы Трисемуса.
46. Шифр Гронсфельда.
47. Система шифрования Вижинера.
48. Шифрование методом Вернама.
49. Методом простой перестановки.
50. Элементы криптоанализа.
51. Современные симметричные системы шифрования.
52. Недостатки симметричных криптосистем.
53. Асимметричные криптосистемы.
54. Принципы асимметричного шифрования.
55. Однонаправленные функции.
56. Алгоритм шифрования RSA.
57. Алгоритм шифрования DES.

58. Шифр ГОСТ 28147.
59. Блочные шифры.
60. Поточные шифры.
61. Проблема обеспечения целостности информации.
62. Функции хэширования
63. Электронно-цифровая подпись.
64. Цифровая подпись в схеме Эль – Гамалья
65. Расширенный метод Евклида.
66. Криптографические протоколы.
67. Классификация криптографических протоколов.
68. Основные элементы криптографических протоколов.
69. Протоколы обмена ключами.
70. Генерация ключей.
71. Защищенные транспортные протоколы.
72. Защищенный протокол HTTPS.

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

Уровень сформированности компетенций			
«Минимальный уровень не достигнут» (менее 60 баллов)	«Минимальный уровень» (60-70 баллов)	«Средний уровень» (71-85 баллов)	«Высокий уровень» (86-100 баллов)
<p><u>Компетенции не сформированы.</u></p> <p>Знания отсутствуют, умения и навыки не сформированы.</p>	<p><u>Компетенции сформированы.</u></p> <p>Сформированы базовые структуры знаний. Умения фрагментарны и носят репродуктивный характер. Демонстрируется низкий уровень самостоятельности практического навыка.</p>	<p><u>Компетенции сформированы.</u></p> <p>Знания обширные, системные. Умения носят репродуктивный характер, применяются к решению типовых заданий. Демонстрируется достаточный уровень самостоятельности устойчивого практического навыка.</p>	<p><u>Компетенции сформированы.</u></p> <p>Знания твердые, аргументированные, всесторонние. Умения успешно применяются к решению как типовых, так и нестандартных творческих заданий. Демонстрируется высокий уровень самостоятельности, высокая адаптивность практического навыка</p>
Описание критериев оценивания			
<p>Обучающийся демонстрирует:</p> <ul style="list-style-type: none"> - существенные пробелы в знаниях учебного материала; - допускаются принципиальные ошибки при ответе на основные вопросы, отсутствует знание и понимание основных 	<p>Обучающийся демонстрирует:</p> <ul style="list-style-type: none"> - знания теоретического материала; - неполные ответы на основные вопросы, ошибки в ответе, недостаточное понимание сущности излагаемых вопросов; 	<p>Обучающийся демонстрирует:</p> <ul style="list-style-type: none"> - знание и понимание основных вопросов контролируемого объема программного материала; - твердые знания теоретического материала. - способность 	<p>Обучающийся демонстрирует:</p> <ul style="list-style-type: none"> - глубокие, всесторонние и аргументированные знания программного материала; - полное понимание сущности и взаимосвязи рассматриваемых

<p>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.</p>	<p>- неуверенные и неточные ответы на дополнительные вопросы; - недостаточное владение литературой, рекомендованной программой дисциплины; - умение без грубых ошибок решать практические задания, которые следует выполнить.</p>	<p>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.</p>	<p>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.</p>
<p>Оценка «неудовлетворительно» / не зачтено</p>	<p>Оценка «удовлетворительно» / «зачтено»</p>	<p>Оценка «хорошо» / «зачтено»</p>	<p>Оценка «отлично» / «зачтено»</p>

9. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

- Голиков, А.М. Защита информации в инфокоммуникационных системах и сетях : учебное пособие / А.М. Голиков ; Томский Государственный университет систем управления и радиоэлектроники (ТУСУР). – Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. – 284 с. : схем., табл., ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=480637> (дата обращения: 06.01.2021). – Библиогр. в кн. – Текст : электронный.
- Алгебраические структуры и их приложения : учебное пособие / Л.В. Зяблицева, С.Ю. Корабельщикова, И.В. Кузнецова, С.А. Тихомиров ; Северный (Арктический) федеральный университет им. М. В. Ломоносова. – Архангельск : Северный

- (Арктический) федеральный университет (САФУ), 2015. – 169 с. : ил., табл. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=436142> (дата обращения: 06.01.2021). – Библиогр. в кн. – ISBN 978-5-261-01074-6. – Текст : электронный.
3. Королев, В.Т. Математика и информатика : учебное пособие / В.Т. Королев, Д.А. Ловцов, В.В. Радионов ; ред. Д.А. Ловцов ; Российский государственный университет правосудия. – Москва : Российский государственный университет правосудия (РГУП), 2015. – Ч. 1. Математика. – 246 с. : ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=439574> (дата обращения: 06.01.2021). – ISBN 978-5-93916-462-7. – Текст : электронный.

б) дополнительная литература:

4. Котова, Л.В. Сборник задач по дисциплине «Методы и средства защиты информации» : учебное пособие / Л.В. Котова ; Московский педагогический государственный университет. – Москва : Московский педагогический государственный университет (МПГУ), 2015. – 44 с. : ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=469877> (дата обращения: 06.01.2021). – Библиогр. в кн. – ISBN 978-5-4263-0221-1. – Текст : электронный.
5. Смирнов, В.И. Защита информации: лабораторный практикум / В.И. Смирнов ; Поволжский государственный технологический университет. – Йошкар-Ола : Поволжский государственный технологический университет, 2017. – 67 с. : ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=476512> (дата обращения: 06.01.2021). – Библиогр. в кн. – ISBN 978-5-8158-1866-8. – Текст : электронный.

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 текстовых заимствований «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 г.

2. Рабочая программа

пересмотрена и актуализирована на заседании кафедры алгебры и геометрии протокол № 7 от 14.03.2019г.;

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 от 24.03.2020г.;

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