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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ «Группы, кольца, алгоритмы и математическое обоснование RSA»

Направление подготовки 01.03.01 Математика

Профиль: "Кибербезопасность"

Форма обучения – очная

Владикавказ 2019

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 10.01.2018 г. № 8, учебным планом подготовки бакалавриата по направлению подготовки 01.03.01 Математика, профиль: "Кибербезопасность", утвержденным Ученым советом ФГБОУ ВО «СГУ» от 28.05.2019 г. № 10.

Составитель: доцент Гутнова А.К.

Рабочая программа обсуждена и утверждена на заседании кафедры алгебры и геометрии .
(протокол № от 14.03.2019)

Одобрена советом факультета математики и информационных технологий
(протокол № от 29.03.2019)

1. Структура и общая трудоемкость дисциплины

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

	Очная Форма обучения
Курс	4
Семестр	7
Лекции	34
Практические занятия	34
Лабораторные занятия	-
Консультации	+
Итого аудиторных занятий	68
Самостоятельная работа	49
Курсовая работа	-
Зачет	-
Экзамен	27
Общее количество часов	144 час.

2. Цели освоения дисциплины

Целью данного курса является систематическое изложение научных основ криптографии от простейших примеров и основных понятий до современных криптографических конструкций. Понимание принципов криптографии стало для многих потребностью в связи с широким распространением криптографических средств обеспечения информационной безопасности.

Задачи дисциплины:

- изучение теоретических принципов криптографии;
- изучение истории криптографии; – изучение криптографических алгоритмов;
- развитие аналитического мышления студентов и повышение их общей математической культуры;
- привить студентам умение самостоятельно изучать учебную и научную литературу

3. Место дисциплины в структуре ОПОП:

Дисциплина «Группы, кольца, алгоритмы и математическое обоснование RSA» относится к дисциплинам Блок 1. Дисциплины (модули). Часть, формируемая участниками образовательных отношений. Дисциплины по выбору. Б1.В.ДВ.06.02.

Для изучения дисциплины необходимы знания, полученные обучающимися в рамках школьного курса математических дисциплин, а также в результате освоения дисциплин: «Алгебра», «Теория чисел».

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):

УК- 1 - Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;

ПК- 3 - Способен проводить научно- исследовательские и опытно-конструкторские разработки по отдельным разделам темы.

Взаимосвязь планируемых результатов обучения по дисциплине с формируемыми компетенциями ОПОП:

Компетенции		**Планируемые результаты обучения, соответствующие формируемым компетенциям ОПОП**		
Код	**Формулировка**	**Знать:**	**Уметь**	**Владеть:**
УК-1	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	требования к шифрам и основные характеристики шифров; принцип работы современных поточных и блочных шифров; принцип работы кодов аутентификации сообщений; принцип работы алгоритмов DES и AES	использовать алгоритмы RSA и Эль-Гамаля для шифрования коротких сообщений; навыками использования ЭВМ в анализе простейших шифров	навыками использования типовых криптографических алгоритмов
ПК-3	Способен проводить научно-исследовательские и опытно-конструкторские разработки по отдельным разделам темы	основные поточные и блочные шифры; основные шифры с открытыми ключами; частотные характеристики открытых текстов и способы их применения к анализу простейших шифров замены и перестановки	синтезировать поточные шифры из регистров сдвига с линейными обратными связями; проводить вычисления в конечных полях	навыком вычислений в арифметике остатков

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			Формы контроля			Литература		
		л	пр	лаб	Содержание	Часы		min	max	
1- 2	Математический аппарат: кольца вычетов, сравнения, и конечные поля.	3	3				Конспект, вопросы на коллоквиуме	**0**	**11**	**[1- 6]**
3- 4	Полная и приведенная система вычетов. Теорема обратимости.	3	3				Конспект, вопросы на коллоквиуме	**0**	**11**	**[1- 6]**
5- 6	Расширенный алгоритм Евклида. Алгебраические структуры на целых числах.	4	4		Политика в сфере обеспечения информационной безопасности России	15	Конспект, вопросы на коллоквиуме	**0**	**11**	**[1- 6]**
7- 8	Теорема Эйлера и ее приложения. Криптосисте	4	4		Использование блочных алгоритмов	14	Конспект, вопросы на коллоквиуме	**0**	**11**	**[1- 6]**

	ма RSA. Теоремы Эйлера и Ферма. Тест Ферма на простоту. Применение теоремы Эйлера в RSA.				шифрования для формирования хеш-функции. Обзор алгоритмов формирования хеш-функций.					
9- 10	Система сравнений первой степени. Китайская теорема об остатках. Применения китайской теоремы об остатках.	4	4				Конспект, вопросы на коллоквиуме	**0**	**11**	**[1- 6]**
11- 12	Сравнения любой степени по составному модулю. Теория квадратичных вычетов.	4	4		Эллиптическая криптография	10	Конспект, вопросы на коллоквиуме	**0**	**11**	**[1- 6]**
13- 14	Первообразные корни и индексы. Порождающий элемент и дискретный	4	4				Конспект, вопросы на коллоквиуме	**0**	**11**	**[1- 6]**

	логарифм.									
15- 16	Построение доказуемо простых чисел общего и специального вида. Алгоритмы в криптографии и криптоанализе.	4	4				Конспект, вопросы на коллоквиуме	**0**	**11**	**[1- 6]**
17- 18	Элементы теории сложности. Алгоритмы факторизации.	4	4		Основные подходы к измерению информации. Энтропия и неопределенность. Норма языка и избыточность сообщений. Понятие совершенно секретной системы. Расстояние единственности	10	Конспект, вопросы на коллоквиуме	**0**	**12**	**[1- 6]**

	ИТОГО	34	34	0		49		**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 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 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. Циклические группы.
2. Пусть $(a,b)=1$. Доказать, что $(a+b,a-b)\leq 2$.

Критерии оценивания представлены в таблице 8.1.

Примеры тестовых заданий по дисциплине:

1) **Инженерно- техническая защита не включает в себя:**
- программные средства
- криптографические средства
- аппаратные средства
- организацию использования технических средств сбора, обработки, накопления и хранения конфиденциальной информации

2) **Укажите, что из перечисленного не является задачей защиты компьютерной информации:**
- обеспечение непрерывности
- обеспечение целостности
- обеспечение доступности
- обеспечение конфиденциальности

3) **На что подразделяется признак классификации угроз «по степени преднамеренности проявления »**
- угрозы доступа к информации на внешних запоминающих устройствах, в оперативной памяти, циркулирующей в линиях связи, отображаемой на терминале или печатаемой на принтере
- угрозы, которые при реализации ничего не меняют в структуре и содержании АС и при воздействии вносят изменения в структуру и содержание АС
- угрозы, вызванные воздействиями на АС и ее компоненты объективных физических процессов или стихийных природных явлений, независящих от человека, и исходящие от человека
- угрозы случайного действия и угрозы преднамеренного действия

4) **На что подразделяется признак классификации угроз «по степени зависимости от активности АС»**
- угрозы, которые могут проявляться на этапе доступа к ресурсам АС и после разрешения доступа к ресурсам АС
- угрозы доступа к информации на внешних запоминающих устройствах, к информации в оперативной памяти, циркулирующей в линиях связи, отображаемой на терминале или печатаемой на принтере
- угрозы, вызванные воздействиями на АС и ее компоненты объективных физических процессов или стихийных природных явлений, независящих от человека, и исходящие от человека
- угрозы, которые могут проявляться независимо от активности АС и проявляться только в процессе функционирования автоматизированной обработки данных

5) **Стандарт шифрования данных DES основан на:**

- преобразовании, реализуемым сетью Фейстеля
- алгоритме сложных математических преобразованиях исходного текста по некоторой формуле
- алгоритме простой замены
- алгоритме шифрования Enigma

6) **Симметричный алгоритм шифрования имеет блоки по 64 бит и основан на 16 кратной перестановке данных, для зашифровывания использует ключ в 56 бит – это шифр:**
- RSA;
- ГОСТ 28147- 89;
- RC2 или RC4;
- DES.

7) **Криптосистема RSA относится к:**
- Одноключевым криптографическим алгоритмам;
- двухключевым криптографическим алгоритмам;
- бесключевым криптографическим алгоритмам;
- может относиться к одноключевым и бесключевым криптографическим алгоритмам.

8) **От какого действия не позволяет защитить данные ЭЦП:**
- Маскарад – абонент С посылает документ абоненту В от имени абонента А;
- Отказ - абонент А заявляет, что не посылал сообщение абоненту В, хотя на самом деле послал;
- Подмена – абонент В изменяет или формирует новый документ и заявляет, что получил его от абонента А;
- нарушение конфиденциальности .

9) **Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, это метод:**
- гаммирования;
- подстановки;
- кодирования;
- перестановки;

10) **Уязвимость типа переполнение буфера основана на:**
- возможности переполнения стека атакуемой подпрограммы
- возможности вставки дополнительных команд в SQL –запросы, приводящих к искажению искомого SQL - запроса к СУБД
- использовании функций с непроверяемым параметром форматирующей строки
- ошибках, допущенными пользователями и администраторами системы в процессе использования общесистемного и прикладного ПО

11) **В правиле Кирхгоффа стойкости шифра полагается, что:**
- Весь механизм криптографических преобразований не известен противнику и надежность алгоритма зависит только от сложности этих преобразований

- Весь механизм криптографических преобразований известен противнику, надежность алгоритма определяется только неизвестным значением секретного ключа
- Надежность криптографического алгоритма не должна определяться только неизвестным значением секретного ключа
- Весь механизм криптографических преобразований не известен противнику, но на надежность алгоритма влияет значение секретного ключа

12) **Метод перебора криптоанализа заключается в:**
- Исследовании статистических закономерностей в появлении комбинаций символов в естественной речи
- Последовательном переборе всего ключевого пространства
- Использовании парадокса дней рождений
- Замене сложных криптографических преобразований, описывающих алгоритм, их приближениями в классе линейных функций.

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 (мах 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 (мах 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.	Правильно выполнена большая часть	Задания выполнены более чем наполовину.	Задания выполнены менее чем наполовину.

		Продемонстрирован высокий уровень владения материалом. Проявлены превосходные способности применять знания и умения к выполнению конкретных заданий.	заданий. Присутствуют незначительные ошибки. Продемонстрирован хороший уровень владения материалом. Проявлены средние способности применять знания и умения к выполнению конкретных заданий.	Присутствуют серьезные ошибки. Продемонстрирован удовлетворительный уровень владения материалом. Проявлены низкие способности применять знания и умения к выполнению конкретных заданий.	Продемонстрирован 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 зачёту:

1. Теория делимости, наибольший общий делитель, непрерывные дроби, простые числа, теорема разложения.
2. Сравнения и классы вычетов.
3. Сравнимость по модулю, функция Эйлера, теорема Эйлера и Ферма.
4. Квадратичные вычеты и невычеты, символы Лежандра и Якоби.
5. Показатели, первообразные корни и дискретный логарифм.
6. Примитивные корни, псевдопростые числа.
7. Структура конечных циклических групп, конечные группы в криптографических системах.
8. Поле классов вычетов по простому модулю, конечные поля в вопросах защиты информации. Примеры криптографических алгоритмов.
9. Криптографические хеш- функции.

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 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	Обучающийся демонстрирует: - знания теоретического материала; - неполные ответы на основные вопросы, ошибки в ответе, недостаточное понимание сущности излагаемых вопросов; - неуверенные и неточные ответы на дополнительные вопросы; - недостаточное владение литературой, рекомендованной программой дисциплины; - умение без	Обучающийся демонстрирует: - знание и понимание основных вопросов контролируемого объема программного 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	Обучающийся демонстрирует: - глубокие, всесторонние и аргументированные знания программного материала; - 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,

дисциплины; - отсутствие готовности (способности) к дискуссии и низкую степень контактности.	грубых ошибок решать практические задания, которые следует выполнить.	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.	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 – Библиогр. в кн. – ISBN 978-5-9275-2501-0. – Текст : электронный.
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 – Текст : электронный.
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 – Текст : электронный.
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 – Текст : электронный.

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 – Библиогр.: с. 213. – Текст : электронный.
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 – Библиогр.: с. 301. – ISBN 978-5-9275-3363-3. – 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 .

– Базаданных «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 04.2016 г);
2. Office Standard 2016 (№ 4100072800 Microsoft Products (MPSA) от 04.2016 г);
3. Система поиска текстовых заимствований «Антиплагиат ВУЗ»;

Перечень ПО в свободном доступе:

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

OperaBrowser .

11. Лист обновления/актуализации

1. 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.