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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Методы криптоанализа»

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: профессор Койбаев В.А.

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

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

1. Структура и общая трудоемкость дисциплины

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

	Очная Форма обучения
Курс	4
Семестр	8
Лекции	38
Практические занятия	38
Лабораторные занятия	-
Консультации	+
Итого аудиторных занятий	76
Самостоятельная работа	41
Курсовая работа	-
Зачет	-
Экзамен	27
Общее количество часов	144 час.

2. Цели освоения дисциплины

Целью курса «Методы криптоанализа» является приобретение студентами знаний о важнейших разделах криптоанализа и сформировать у студентов достаточно глубокие знания о:

- моделях угроз;
- криптоанализе исторических шифров;
- основных методах современного криптоанализа и возможностях его применения.

Задачи дисциплины:

- изучение основных определений и принципов криптоанализа, которые необходимы для успешного усвоения методов взлома криптографических алгоритмов;
- изучение основных моделей угроз, применяемых в криптоанализе;
- овладение навыками криптоанализа симметричных и асимметричных криптографических алгоритмов;
- привить студентам умение самостоятельно изучать учебную литературу и научные публикации по криптоанализу.

3. Место дисциплины в структуре ОПОП:

Дисциплина «Методы криптоанализа» относится к дисциплинам Блок 1. Дисциплины (модули). Вариативная часть. Дисциплины по выбору. Б1.В.ДВ.10.02.

Для изучения дисциплины необходимы знания, полученные обучающимися в рамках школьного курса математических дисциплин, курса «Информатика», а также в результате освоения дисциплин: «Компьютерные науки (Информатика)», «Компьютерные науки (Практикум на ПК)».

Приступая к изучению дисциплины «Методы криптоанализа», студент должен иметь представление о теории чисел, алгебре, теории вероятностей.

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-2 -способностью математически корректно ставить естественнонаучные задачи, знание постановок классических задач математики;

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 вероятносте	основные понятия и методы криптоанализа;	оценивать стойкость современных криптографических алгоритмов по отношению к методам криптоанализа;	криптографической терминологией;

	й, математической статистики и случайных процессов, численных методов, теоретической механики в будущей профессиональной деятельности			
ОПК-3	способностью к самостоятельной научно-исследовательской работе	частотные характеристики открытых текстов и способы их применения к анализу простейших шифров замены и перестановки;	применять математические методы исследования моделей шифров	современными методами криптоанализа
ПК-2	способностью математически корректно ставить естественнонаучные задачи, знание постановок классических задач математики	модели шифров и математические методы их исследования	строить современные шифрсистемы	криптографической терминологией; методами крипто-анализа простейших шифров;
ПК-3	способностью строго доказать утверждение, сформулировать результат, увидеть следствия полученного результата	основные принципы построения криптоалгоритмов; основные методы дешифрования; стандарты систем шифрования	формулировать постановки задач криптоанализа и находить подходы к их решению	современной научнотехнической литературой в области криптографической защиты

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	лаб	Содержание	Часы		min	max	
1-2	Общие понятия криптоанализа	4	4				Конспект, вопросы на коллоквиуме	**0**	**10**	**[1-6]**
3-4	Криптоанализ исторических шифров	4	4				Конспект, вопросы на коллоквиуме	**0**	**10**	**[1-6]**
5-6	Криптоанализ поточных шифров	5	5		Методы вычисления дискретного логарифма в группе точек эллиптической кривой над конечным полем	15	Конспект, вопросы на коллоквиуме	**0**	**10**	**[1-6]**
7-8	Криптоанализ блочных шифров	5	5				Конспект, вопросы на коллоквиуме	**0**	**10**	**[1-6]**
9-10	Поиск коллизий хеш-функций	5	5				Конспект, вопросы на коллоквиуме	**0**	**15**	**[1-6]**
11-13	Криптоанализ алгоритма RSA	5	5		Алгебраический криптоанализ ГОСТ 28147-89.	15	Конспект, вопросы на коллоквиуме	**0**	**15**	**[1-6]**
14-16	Криптоанализ алгоритмов, основанных на использовании дискретного-логарифма в конечном поле	5	5		Акустический криптоанализ	11	Конспект, вопросы на коллоквиуме	**0**	**15**	**[1-6]**
17-18	Квантовые атаки на криптосистемы с открытым ключом	5	5				Конспект, вопросы на коллоквиуме	**0**	**15**	**[1-6]**

	ИТОГО	38	38	0		41		**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. принципы работы криптографических хеш-функций
2. Разработать программу взлома шифра Виженера с помощью частотного анализа

Критерии оценивания представлены в таблице 8.1.

Примеры тестовых заданий по дисциплине:

Что в переводе с греческого языка означает слово «криптография»?

- шифр
- тайнопись
- преобразование
- расшифровка

Как называется «исторический» шифр, в котором каждая буква исходного текста заменялась буквой, стоящей на некоторое фиксированное число мест дальше в алфавите, о применении которого имеются документальные свидетельства?

- шифр Маркова
- шифр Цезаря
- шифр Энигма
- шифр Бэбиджа

Когда в криптографии стало использоваться асимметричное шифрование?

- в первой половине XIX;
- во второй половине XIX;
- в первой половине XX;
- во второй половине XX

Как называется совокупность заранее оговоренных способов преобразования исходного секретного сообщения с целью его защиты?

- алгоритм
- ключ
- протокол
- шифр

Как называется сообщение, полученное после преобразования с использованием любого шифра?

- закрытым текстом
- имитовставкой
- ключом
- открытым текстом

Что в криптографии называют открытым текстом?

- исходное сообщение (сообщение до шифрования)
- открытый ключ шифрования
- сообщение, получение после преобразования с использованием любого шифра
- электронную цифровую подпись

Гарантирование невозможности несанкционированного изменения информации - это:

- обеспечение целостности
- обеспечение конфиденциальности
- обеспечение аутентификации
- обеспечение шифрования

Под конфиденциальностью понимают (выберите продолжение)

- решение проблемы защиты информации от ознакомления с ее содержанием со стороны лиц, имеющих права доступа к ней
- решение проблемы защиты информации от ознакомления с ее содержанием со стороны лиц, не имеющих права доступа к ней

- решение проблемы защиты информации от ее изменения со стороны лиц, не имеющих права доступа к ней
- решение проблемы запуска программ со стороны лиц, не имеющих права доступа к ним
- разрешение пользоваться информацией только одному лицу

Под целостностью понимают (выберите продолжение)
- гарантирование невозможности несанкционированного изменения объема информации
- гарантирование невозможности несанкционированного изменения информации
- гарантирование невозможности несанкционированного изменения порядка следования информации
- гарантирование невозможности несанкционированного изменения переносов в текстовой информации

Выберите правильное определение термина «криптоанализ»
- криптоанализ – это наука о преодолении криптографической защиты информации
- криптоанализ – это наука, занимающаяся шифрованием данных при передаче по открытым каналам связи
- криптоанализ изучает построение и использование систем шифрования, в том числе их стойкость, слабости и степень уязвимости относительно различных методов вскрытия
- криптоанализ изучает способы защиты информации, основанные на попытке скрыть от противника сам факт наличия интересующей его информации

Какая наука разрабатывает методы «вскрытия» шифров?
- криптография
- криптоанализ
- теория чисел
- тайнопись
- линейная алгебра

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,	Тема полностью	Тема в основном	Тема частично	Тема не раскрыта.

	презентация (max 3б.) / опорный конспект (max 2б.)	раскрыта. Превосходное владение материалом. Высокий уровень самостоятельности, логичности, аргументированности. Превосходный стиль изложения.	раскрыта. Хорошее владение материалом. Средний уровень самостоятельности, логичности, аргументированности. Хороший стиль изложения.	раскрыта. Удовлетворительное владение материалом. Низкий уровень самостоятельности, логичности, аргументированности. Удовлетворительный стиль изложения.	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 заданий.	Задания выполнены менее чем наполовину. 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 экзамену:

1. Общие понятия криптоанализа

2. Криптоанализ исторических шифров
3. Криптоанализ поточных шифров
4. Криптоанализ блочных шифров
5. Поиск коллизий хеш-функций
6. Криптоанализ алгоритма RSA
7. Криптоанализ алгоритмов, основанных на использовании дискретного-логарифма в конечном поле
8. Квантовые атаки на криптосистемы с открытым ключом

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	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	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;	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

выполнять практические задания, предусмотренные программой дисциплины; - отсутствие готовности (способности) к дискуссии и низкую степень контактности.	программой дисциплины; - умение без грубых ошибок решать практические задания, которые следует выполнить.	- 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.	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. Алексеев, Д.М. Разработка и исследование параллельных алгоритмов криптоанализа симметричного блочного шифра Магма: выпускная квалификационная (дипломная) работа / Д.М. Алексеев ; Южный федеральный университет, Институт компьютерных технологий и информационной безопасности, Кафедра Безопасности информационных технологий. – Таганрог : , 2017. – 74 с. : схем., ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=463137 – Текст : электронный.
2. Котов, Ю.А. Приложения шифров: криптоанализ : [16+] / Ю.А. Котов ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2019. – 76 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=575479 – Библиогр.: с. 44. – ISBN 978-5-7782-3902-9. – Текст : электронный.
3. Куттубек, к.Г. Применение методов искусственного интеллекта в криптоанализе шифра Плейфера / к.Г. Куттубек ; Национальный исследовательский Томский государственный университет (НИ ТГУ). – Томск : б.и., 2020. – 28 с. : ил., граф. –

Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=597089 – Текст : электронный.

4. Ниссенбаум, О.В. Теоретико-числовые методы в криптографии. Сборник заданий: учебно-методическое пособие для студентов специальностей «Компьютерная безопасность» и «Информационная безопасность автоматизированных систем», направления «Информационная безопасность» : [16+] / О.В. Ниссенбаум ; Тюменский государственный университет. – Тюмень : Тюменский государственный университет, 2014. – Ч. 3. – 40 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=567498 – Библиогр. в кн. – Текст : электронный.

б) дополнительная литература:

5. Гультяева, Т.А. Основы теории информации и криптографии: конспект лекций / Т.А. Гультяева ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2010. – 88 с. : табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=228963 – ISBN 978-5-7782-1425-5. – Текст : электронный.
6. Лапонина, О.Р. Криптографические основы безопасности / О.Р. Лапонина. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 244 с. : ил. – (Основы информационных технологий). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=429092 – Библиогр. в кн. – ISBN 5-9556-00020-5. – 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;
6. Visual Studio 2019.

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.