Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

УТВЕРЖДАЮ
Директор по образовательной
деятельности

_____ С.Т. Князев
«___» _____

РАБОЧАЯ ПРОГРАММА МОДУЛЯ

Код модуля	Модуль
1157325	Математические основы криптографии

Екатеринбург

Перечень сведений о рабочей программе модуля	Учетные данные
Образовательная программа 1. Математические методы защиты информации	**Код ОП** 1. 10.05.01/22.01
Направление подготовки 1. Компьютерная безопасность	**Код направления и уровня подготовки** 1. 10.05.01

Программа модуля составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Ананичев Дмитрий Сергеевич	кандидат физико-математических наук, доцент	Доцент	алгебры и фундаментальной информатики

Согласовано:

Управление образовательных программ Р.Х. Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ Математические основы криптографии

1.1. Аннотация содержания модуля

Модуль состоит из трех дисциплин «Теория чисел», «Теория конечных полей» и «Теоретико-числовые методы в криптографии». Цель изучения данных дисциплин — дать студентам фундаментальные знания о математических понятиях, конструкциях, алгоритмах и алгоритмических проблемах, на основе которых строятся современные технологии защиты информации

1.2. Структура и объем модуля

Таблица 1

№ п/п	Перечень дисциплин модуля в последовательности их освоения	Объем дисциплин модуля и всего модуля в зачетных единицах
1	Теория конечных полей	2
2	Теория чисел	2
3	Теоретико-числовые методы в криптографии	4
	ИТОГО по модулю:	8

1.3.Последовательность освоения модуля в образовательной программе

Пререквизиты модуля	Не предусмотрены
Постреквизиты и кореквизиты модуля	Не предусмотрены

1.4. Распределение компетенций по дисциплинам модуля, планируемые результаты обучения (индикаторы) по модулю

Таблица 2

Перечень дисциплин модуля	Код и наименование компетенции	Планируемые результаты обучения (индикаторы)
1	2	3
Теоретико-числовые методы в криптографии	ОПК-3 - Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения	З-1 - Описывать математические методы, необходимые для решения задач профессиональной деятельности У-1 - Выбирать математические методы и модели для решения задач профессиональной деятельности

	задач профессиональной деятельности	П-1 - Иметь практический опыт решения математических задач в области профессиональной деятельности
	ОПК-8 - Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей	З-1 - Описывать основные перспективы развития науки и техники в области профессиональной деятельности У-1 - Формулировать задачи исследования, выбирать методы и средства их решения П-1 - Иметь практический опыт решения теоретических задач в областях математики
	ОПК-10 - Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности	З-4 - Описывать основные конструкции, используемые в построении современных симметричных шифров и криптографических хеш-функций, и их свойства З-5 - Описывать устройство современных блочных шифров, поточных шифров и криптографических хэш-функций У-4 - Реализовывать алгоритмы для работы с современными асимметричными криптосистемами и подписями на их основе
	ОПК-18 - Способен разрабатывать алгоритмы, реализующие современные математические методы защиты информации	З-3 - Описывать понятия временной и пространственной сложности алгоритма, его зависимость от модели вычисления З-8 - Описывать основные конструкции, используемые в построении современных симметричных шифров и криптографических хеш-функций, и их свойства У-1 - Оценивать механизмы защиты, реализующие криптографические протоколы У-4 - Реализовывать алгоритмы для работы с современными асимметричными криптосистемами и подписями на их основе П-1 - Иметь практический опыт деятельности по оценке вычислительной сложности алгоритмических проблем
	ОПК-19 - Способен разрабатывать и анализировать математические модели	З-4 - Описывать основные конструкции, используемые в построении современных симметричных шифров и

	механизмов защиты информации	криптографических хеш-функций, и их свойства У-1 - Выбирать математические методы и модели для решения задач профессиональной деятельности П-1 - Иметь практический опыт решения математических задач в области профессиональной деятельности
Теория конечных полей	ОПК-3 - Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности	З-1 - Описывать математические методы, необходимые для решения задач профессиональной деятельности У-1 - Выбирать математические методы и модели для решения задач профессиональной деятельности П-1 - Иметь практический опыт решения математических задач в области профессиональной деятельности
	ОПК-8 - Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей	З-1 - Описывать основные перспективы развития науки и техники в области профессиональной деятельности У-1 - Формулировать задачи исследования, выбирать методы и средства их решения П-1 - Иметь практический опыт решения теоретических задач в областях математики
	ОПК-10 - Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности	З-4 - Описывать основные конструкции, используемые в построении современных симметричных шифров и криптографических хеш-функций, и их свойства З-5 - Описывать устройство современных блочных шифров, поточных шифров и криптографических хэш-функций
	ОПК-18 - Способен разрабатывать алгоритмы, реализующие современные математические методы защиты информации	З-8 - Описывать основные конструкции, используемые в построении современных симметричных шифров и криптографических хеш-функций, и их свойства

		З-9 - Описывать устройство современных блочных шифров, поточных шифров и криптографических хэш-функций
	ОПК-19 - Способен разрабатывать и анализировать математические модели механизмов защиты информации	З-4 - Описывать основные конструкции, используемые в построении современных симметричных шифров и криптографических хеш-функций, и их свойства У-1 - Выбирать математические методы и модели для решения задач профессиональной деятельности П-1 - Иметь практический опыт решения математических задач в области профессиональной деятельности
Теория чисел	ОПК-3 - Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности	З-1 - Описывать математические методы, необходимые для решения задач профессиональной деятельности У-1 - Выбирать математические методы и модели для решения задач профессиональной деятельности П-1 - Иметь практический опыт решения математических задач в области профессиональной деятельности
	ОПК-8 - Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей	З-1 - Описывать основные перспективы развития науки и техники в области профессиональной деятельности У-1 - Формулировать задачи исследования, выбирать методы и средства их решения П-1 - Иметь практический опыт решения теоретических задач в областях математики
	ОПК-19 - Способен разрабатывать и анализировать математические модели механизмов защиты информации	У-1 - Выбирать математические методы и модели для решения задач профессиональной деятельности П-1 - Иметь практический опыт решения математических задач в области профессиональной деятельности

1.5. Форма обучения

Обучение по дисциплинам модуля может осуществляться в очной формах.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Теория конечных полей

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Баранский Виталий Анатольевич	доктор физико-математических наук, профессор	Профессор	алгебры и фундаментальной информатики

Рекомендовано учебно-методическим советом института Естественных наук и математики

Протокол № _1_ от _21.10.2021_ г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

- **Баранский Виталий Анатольевич, Профессор, алгебры и фундаментальной информатики**

1.1. Технологии реализации, используемые при изучении дисциплины модуля

- Традиционная (репродуктивная) технология
- Разноуровневое (дифференцированное) обучение
  - Базовый уровень

**Базовый I уровень – сохраняет логику самой науки и позволяет получить упрощенное, но верное и полное представление о предмете дисциплины, требует знание системы понятий, умение решать проблемные ситуации. Освоение данного уровня результатов обучения должно обеспечить формирование запланированных компетенций и позволит обучающемуся на минимальном уровне самостоятельности и ответственности выполнять задания;*
Продвинутый II уровень – углубляет и обогащает базовый уровень как по содержанию, так и по глубине проработки материала дисциплины. Это происходит за счет включения дополнительной информации. Данный уровень требует умения решать проблемы в рамках курса и смежных курсов посредством самостоятельной постановки цели и выбора программы действий. Освоение данного уровня результатов обучения позволит обучающемуся повысить уровень самостоятельности и ответственности до творческого применения знаний и умений.

1.2. Содержание дисциплины

Таблица 1.1

Код раздела, темы	Раздел, тема дисциплины*	Содержание
Р1	Расширения полей.	Вложение областей целостности в поля. Поле рациональных дробей. Китайская теорема об остатках. Алгебраический расширения полей. Конечные расширения полей, алгебраические и трансцедентные элементы, минимальный многочлен, простое расширение поля. Поле разложения многочлена, существование и единственность.
Р2	Конечные поля и неприводимые многочлены.	Характеризация конечных полей, подполя конечного поля, поле GF(p^k), примитивные элементы и примитивные многочлены. Корни неприводимых многочленов, автоморфизм Фробениуса, сопряженные элементы. Группа автоморфизмов конечного поля.
Р3	Вычисления в конечных полях.	Формула обращения Мёбиуса. Корни из единицы и круговые многочлены, формулы для вычисления круговых многочленов, разложение кругового многочлена на неприводимые множители. Представление элементов в конечных полях, таблицы индексов и примитивные элементы, представление конечных полей матрицами. Многочлены без кратности неприводимых множителей, алгоритм Берлекэмпа разложения многочлена на неприводимые множители. Порядок многочлена, характеризация примитивных многочленов. Методы построения минимальных многочленов. Методы построения примитивных многочленов. Семейство нормированных неприводимых многочленов данной степени

		над конечным полем, Iq(n) и I(q; n; x), разложение многочлена I(q; n; x) в произведение круговых многочленов.

1.3. Направление, виды воспитательной деятельности и используемые технологии

Таблица 1.2

Направление воспитательной деятельности	Вид воспитательной деятельности	Технология воспитательной деятельности	Компетенция	Результаты обучения
Профессиональное воспитание	учебно-исследовательская, научно-исследовательская	Технология формирования уверенности и готовности к самостоятельной успешной профессиональной деятельности	ОПК-19 - Способен разрабатывать и анализировать математические модели механизмов защиты информации	У-1 - Выбирать математические методы и модели для решения задач профессиональной деятельности

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Теория конечных полей

Электронные ресурсы (издания)

1. Ленг, С., С.; Алгебра; Наука, Москва; 1965; https://biblioclub.ru/index.php?page=book&id=464071 (Электронное издание)

Печатные издания

1. Баранский, В. А.; Общая алгебра и ее приложения : [учеб. пособие для вузов].; Изд-во Урал. ун-та, Екатеринбург; 2008 (99 экз.)

2. Лидл, Р.; Прикладная абстрактная алгебра : Учеб. пособие.; Изд-во Урал. ун-та, Екатеринбург; 1996 (49 экз.)

3. Варден, Б. Л. ван дер, Бельский, А. А.; Алгебра; Лань, Санкт-Петербург; 2004 (25 экз.)

Профессиональные базы данных, информационно-справочные системы

Кабанов, Владислав Владимирович. Учебно-методический комплекс дисциплины "Конечные поля" [Электронный ресурс] / В. В. Кабанов ; Федер. агентство по образованию, Урал. гос. ун-т им. А. М. Горького, ИОНЦ "Информационная безопасность" [и др.]. — Электрон. дан. (1,15 Мб). — Екатеринбург : [б. и.], 2008. — 1 электрон. опт. диск (CD-ROM). — Загл. с этикетки диска. — <URL: http://elar.urfu.ru/handle/10995/1657>.

Материалы для лиц с ОВЗ

Весь контент ЭБС представлен в виде файлов специального формата для воспроизведения синтезатором речи, а также в тестовом виде, пригодном для прочтения с использованием экранной лупы и настройкой контрастности.

Базы данных, информационно-справочные и поисковые системы

Общероссийский математический портал http://www.mathnet.ru/

Научная электронная библиотека eLibrary.ru http://www.elibrary.ru/

Сайт издательства Elsevier http://www.sciencedirect.com/

Сайт кафедры: http://kma.imkn.urfu.ru

Сайт кафедры: http://kadm.imkn.urfu.ru/pages.php?id=index

Сайт библиотеки университета http://lib.urfu.ru/

3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Теория конечных полей

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием и программным обеспечением

Таблица 3.1

№ п/п	Виды занятий	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения
1	Лекции	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Подключение к сети Интернет	Office Professional 2003 Win32 Russian CD-ROM Свободное ПО:Google Crome
2	Консультации	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная	**Не требуется**
3	Текущий контроль и промежуточная аттестация	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная	**Не требуется**

4	Самостоятельная работа студентов	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Подключение к сети Интернет	Office Professional 2003 Win32 Russian CD-ROM Свободное ПО:Google Crome

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Теория чисел

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Сизый Сергей Викторович	доктор технических наук, доцент	Профессор	алгебры и фундаментальной информатики

Рекомендовано учебно-методическим советом института Естественных наук и математики

Протокол № _1_ от _21.10.2021_ г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

- **Сизый Сергей Викторович, Профессор, алгебры и фундаментальной информатики**

1.1. Технологии реализации, используемые при изучении дисциплины модуля

- Традиционная (репродуктивная) технология
- Разноуровневое (дифференцированное) обучение
  - Базовый уровень

**Базовый I уровень – сохраняет логику самой науки и позволяет получить упрощенное, но верное и полное представление о предмете дисциплины, требует знание системы понятий, умение решать проблемные ситуации. Освоение данного уровня результатов обучения должно обеспечить формирование запланированных компетенций и позволит обучающемуся на минимальном уровне самостоятельности и ответственности выполнять задания;*
Продвинутый II уровень – углубляет и обогащает базовый уровень как по содержанию, так и по глубине проработки материала дисциплины. Это происходит за счет включения дополнительной информации. Данный уровень требует умения решать проблемы в рамках курса и смежных курсов посредством самостоятельной постановки цели и выбора программы действий. Освоение данного уровня результатов обучения позволит обучающемуся повысить уровень самостоятельности и ответственности до творческого применения знаний и умений.

1.2. Содержание дисциплины

Таблица 1.1

Код раздела, темы	Раздел, тема дисциплины*	Содержание
Р1	Основные понятия и теоремы.	Деление с остатком. Наибольший общий делитель. Взаимно простые числа. Простые числа и основная теорема арифметики. Распределение простых чисел. Алгоритм Евклида. Линейные диофантовы уравнения.
Р2	Цепные дроби.	Разложение чисел в цепные дроби. Вычисление подходящих дробей. Свойства подходящих дробей. Континуанты, их связь с цепными дробями. Анализ алгоритма Евклида. Приближение чисел цепными дробями. Периодичность цепных дробей. Теорема Эрмита.
Р3	Важнейшие функции в теории чисел.	Целая и дробная части. Мультипликативные функции и их основные свойства. Примеры мультипликативных функций. Дзета-функция Римана, ее свойства и применения.
Р4	Теория сравнений.	Определения и простейшие свойства сравнений. Полная и приведенная системы вычетов. Теорема Эйлера и теорема Ферма. Сравнения первой степени. Сравнения любой степени по простому модулю. Сравнения любой степени по составному модулю. Сравнения второй степени, символ Лежандра, его свойства. Закон взаимности Гаусса.
Р5	Трансцендентные числа.	Мера и категория на прямой. Числа Лиувилля. Алгебраические числа, их свойства. Трансцендентность числа е. Трансцендентность числа пи. Трансцендентность значений показательной функции, теорема Линдемана.

1.3. Направление, виды воспитательной деятельности и используемые технологии

Таблица 1.2

Направление воспитательной деятельности	Вид воспитательной деятельности	Технология воспитательной деятельности	Компетенция	Результаты обучения
Профессиональное воспитание	учебно-исследовательская, научно-исследовательская	Технология формирования уверенности и готовности к самостоятельной успешной профессиональной деятельности	ОПК-3 - Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности	У-1 - Выбирать математические методы и модели для решения задач профессиональной деятельности

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Теория чисел

Электронные ресурсы (издания)

1. Сизый, С. В.; Лекции по теории чисел : учебное пособие.; Физматлит, Москва; 2008; https://biblioclub.ru/index.php?page=book&id=68386 (Электронное издание)

2. Виноградов, И. М., Рывкин, А. Э.; Основы теории чисел : учебник.; Государственное издательство технико-теоретической литературы, Москва, Ленинград; 1952; https://biblioclub.ru/index.php?page=book&id=449924 (Электронное издание)

3. Хассе, Г., Г.; Лекции по теории чисел; Иностранная литература, Москва; 1953; https://biblioclub.ru/index.php?page=book&id=454847 (Электронное издание)

4. Хинчин, А. Я., Чернышева, Л. Ю.; Цепные дроби; Государственное издательство физико-математической литературы, Москва; 1960; https://biblioclub.ru/index.php?page=book&id=449480 (Электронное издание)

Профессиональные базы данных, информационно-справочные системы

Арнольд, В.И. Цепные дроби : учеб. пособие — Москва : МЦНМО, 2009. — 40 с.

https://www.mccme.ru/free-books/mmmf-lectures/book.14-full.pdf

Материалы для лиц с ОВЗ

Весь контент ЭБС представлен в виде файлов специального формата для воспроизведения синтезатором речи, а также в тестовом виде, пригодном для прочтения с использованием экранной лупы и настройкой контрастности.

Базы данных, информационно-справочные и поисковые системы

Общероссийский математический портал http://www.mathnet.ru/

Научная электронная библиотека eLibrary.ru http://www.elibrary.ru/

Сайт издательства Elsevier http://www.sciencedirect.com/

Сайт кафедры: http://kma.imkn.urfu.ru

Сайт кафедры: http://kadm.imkn.urfu.ru/pages.php?id=index

Сайт библиотеки университета http://lib.urfu.ru/

3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Теория чисел

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием и программным обеспечением

Таблица 3.1

№ п/п	Виды занятий	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения
1	Лекции	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Периферийное устройство Подключение к сети Интернет	Office Professional 2003 Win32 Russian CD-ROM Свободное ПО:Google Crome
2	Консультации	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная	**Не требуется**
3	Текущий контроль и промежуточная аттестация	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя	**Не требуется**

		Доска аудиторная	
4	Самостоятельная работа студентов	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Подключение к сети Интернет	Office Professional 2003 Win32 Russian CD-ROM Свободное ПО:Google Crome

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Теоретико-числовые методы в криптографии

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Ананичев Дмитрий Сергеевич	кандидат физико-математических наук, доцент	Доцент	алгебры и фундаментальной информатики

Рекомендовано учебно-методическим советом института Естественных наук и математики

Протокол № _1_ от _21.10.2021_ г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

- **Ананичев Дмитрий Сергеевич, Доцент, алгебры и фундаментальной информатики**

1.1. Технологии реализации, используемые при изучении дисциплины модуля

- Традиционная (репродуктивная) технология
- Разноуровневое (дифференцированное) обучение
  - Базовый уровень

**Базовый I уровень – сохраняет логику самой науки и позволяет получить упрощенное, но верное и полное представление о предмете дисциплины, требует знание системы понятий, умение решать проблемные ситуации. Освоение данного уровня результатов обучения должно обеспечить формирование запланированных компетенций и позволит обучающемуся на минимальном уровне самостоятельности и ответственности выполнять задания;*
Продвинутый II уровень – углубляет и обогащает базовый уровень как по содержанию, так и по глубине проработки материала дисциплины. Это происходит за счет включения дополнительной информации. Данный уровень требует умения решать проблемы в рамках курса и смежных курсов посредством самостоятельной постановки цели и выбора программы действий. Освоение данного уровня результатов обучения позволит обучающемуся повысить уровень самостоятельности и ответственности до творческого применения знаний и умений.

1.2. Содержание дисциплины

Таблица 1.1

Код раздела, темы	Раздел, тема дисциплины*	Содержание
P1	Сложность арифметических операций.	Свойства функции сложности. Сложность операций с целыми числами. Сложность алгоритма Евклида. Дискретное преобразование Фурье. Умножение и деление многочленов.
P2	Проверка чисел на простоту.	Элементарные методы. Тест на основе малой теоремы Ферма. Числа Кармайкла. Эйлеровы псевдопростые числа. Тест Соловея-Штрассена. Сильнопсевдопростые числа. Тест Рабина-Миллера. Тест Агравала-КайалаСаксены и его модификация Ленстры-Померанца
P3	Построение больших простых чисел.	Критерий Люка. Понятие сертификата простоты. Теорема Поклингтона. Метод Маурера. (n+1)-методы построения простых чисел.
P4	Факторизация.	(p-1)-метод Полларда. ро-метод Полларда. Метод Полларда-Штрассена. Метод Ферма. Алгоритм Диксона. Модификация Билхарта-Моррисона. Метод квадратичного решета. Алгоритмы решета числового поля.
P5	Дискретное логарифмирование.	Детерминированные методы. ро-метод Полларда. Дискретное логарифмирование в простых полях: алгоритмы Адлемана и Копперсмита-Одлыжко-Шреппеля. Алгогитм исчисления индексов.
P6	Эллиптические кривые.	Свойства эллиптических кривых. Алгоритм Ленстры для факторизации с помощью эллиптических кривых.

		Тестирование чисел на простоту с помощью эллиптических кривых.

1.3. Направление, виды воспитательной деятельности и используемые технологии

Таблица 1.2

Направление воспитательной деятельности	Вид воспитательной деятельности	Технология воспитательной деятельности	Компетенция	Результаты обучения
Профессиональное воспитание	учебно-исследовательская, научно-исследовательская	Технология формирования уверенности и готовности к самостоятельной успешной профессиональной деятельности	ОПК-19 - Способен разрабатывать и анализировать математические модели механизмов защиты информации	У-1 - Выбирать математические методы и модели для решения задач профессиональной деятельности

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Теоретико-числовые методы в криптографии

Электронные ресурсы (издания)

1. Василенко, О. Н.; Теоретико-числовые алгоритмы в криптографии (2-е издание, дополненное) : монография.; МЦНМО, Москва; 2006; https://biblioclub.ru/index.php?page=book&id=61814 (Электронное издание)

2. ; Теоретико-числовые методы в криптографии : практикум.; Северо-Кавказский Федеральный университет (СКФУ), Ставрополь; 2017; https://biblioclub.ru/index.php?page=book&id=483838 (Электронное издание)

Профессиональные базы данных, информационно-справочные системы

Черемушкин А.В. Лекции по арифметическим алгоритмам в криптографии. - М., МЦНМО, 2002. http://window.edu.ru/resource/004/24004/files/cherem.pdf

Материалы для лиц с ОВЗ

Весь контент ЭБС представлен в виде файлов специального формата для воспроизведения синтезатором речи, а также в тестовом виде, пригодном для прочтения с использованием экранной лупы и настройкой контрастности.

Базы данных, информационно-справочные и поисковые системы

Общероссийский математический портал http://www.mathnet.ru/

Научная электронная библиотека eLibrary.ru http://www.elibrary.ru/

Сайт издательства Elsevier http://www.sciencedirect.com/

Сайт кафедры: http://kma.imkn.urfu.ru

Сайт кафедры: http://kadm.imkn.urfu.ru/pages.php?id=index

Сайт библиотеки университета http://lib.urfu.ru/

3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Теоретико-числовые методы в криптографии

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием и программным обеспечением

Таблица 3.1

№ п/п	Виды занятий	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения
1	Лекции	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Периферийное устройство Подключение к сети Интернет	Office Professional 2003 Win32 Russian CD-ROM Свободное ПО:Google Crome
2	Практические занятия	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная	**Не требуется**
3	Консультации	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная	**Не требуется**
4	Текущий контроль и промежуточная аттестация	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная	**Не требуется**

5	Самостоятельная работа студентов	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Периферийное устройство	Office Professional 2003 Win32 Russian CD-ROM Свободное ПО:Google Crome