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
1157338	Специальные главы математики

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 Специальные главы математики

1.1. Аннотация содержания модуля

Модуль состоит из трех дисциплин «Теория кодирования», «Методы алгебраической геометрии» и «Теория псевдослучайных генераторов». 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	Методы алгебраической геометрии	2
2	Теория кодирования	2
3	Теория псевдослучайных генераторов	2
	ИТОГО по модулю:	6

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
Методы алгебраической геометрии	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 У-4 - Реализовывать алгоритмы для работы с современными асимметричными криптосистемами и подписями на их основе
	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 кодирования	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
Теория псевдослучайных генераторов	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

	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

1.5. Форма обучения

Обучение по дисциплинам модуля может осуществляться в очной формах.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Методы алгебраической геометрии

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 № _7_ 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
Р1	Кубическая кривая на плоскости.	Определения. Сложение точек. Теорема о 9 точках.
Р2	Проективная плоскость.	Определения п.плоскости и геометрических объектов в ней. Особые точки кривой и их влияние на операцию сложения точек. Формула Эйлера.
Р3	Нормальные формы неособой кубической кривой.	Вывод нормальных форм над полем характеристики >3. Выводы нормальных форм над полями характеристик 2 и 3. Вывод условия отсутствия особых точек для кривых в нормальной форме.
Р4	Сложение точек.	Вывод формул для сложения точек на кривых в нормальных формах
Р5	Теорема Хассе.	Доказательство Манина теоремы Хассе.

1.3. Направление, виды воспитательной деятельности и используемые технологии

Таблица 1.2

Направление воспитательной	Вид воспитательной	Технология воспитательной	Компетенция	Результаты обучения

деятельности	деятельности	деятельности		
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

Методы алгебраической геометрии

Электронные ресурсы (издания)

1. Шафаревич, И. Р.; Основы алгебраической геометрии : монография.; МЦНМО, Москва; 2007; https://biblioclub.ru/index.php?page=book&id=63255 (Электронное издание)

2. Ходж, В. В., Узков, А. И.; Методы алгебраической геометрии : монография.; Изд-во иностр. лит., Москва; 1954; https://biblioclub.ru/index.php?page=book&id=255667 (Электронное издание)

Профессиональные базы данных, информационно-справочные системы

1. J.H.Silverman, The Arithmetic of Elliptic Curves.- Spriger 2009. DOI: 10.1007/978-0-387-09494-6

https://link.springer.com/content/pdf/10.1007%2F978-0-387-09494-6.pdf

2. 2. FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Digital Signature Standard (DSS) NIST FIPS PUB 186-4

https://csrc.nist.gov/CSRC/media/Publications/fips/186/3/archive/2009-06-25/documents/fips_186-3.pdf

3. 2. Ю.Г. Прохоров, Эллиптические кривые и криптография.

https://homepage.mi-ras.ru/~prokhoro/teach/crypt.pdf

4. 1. Ю. И. Манин, О сравнениях третьей степени по простому модулю, Изв. АН СССР. Сер.

матем., 1956, том 20, выпуск 5, 673–678

http://www.mathnet.ru/links/2ebfad28884637379b23881879557af7/im3844.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

Методы алгебраической геометрии

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 Периферийное устройство Подключение к сети Интернет	Office Professional 2003 Win32 Russian CD-ROM Свободное ПО:Google Crome
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 Подключение к сети Интернет	Office Professional 2003 Win32 Russian CD-ROM Свободное ПО:Google Crome

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Теория кодирования

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 № _7_ 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
Р1	Модель канала без памяти.	Математическая модель, изучаемая теорией кодирования: двоичный симметричный канал без памяти. Обсуждение модели. Теорема Шеннона.
Р2	Основные параметры кодов, исправляющих ошибки.	Длина, скорость, минимальное расстояние. Связь между минимальным расстоянием и корректирующими возможностями кода. Граница Хэмминга. Совершенные коды.
Р3	Линейные коды.	Порождающая матрица. Граница Синглтона. Граница Плоткина. Граница Элайса. Дуальный код. Контрольная матрица. Код Хэмминга. Характеризация минимального расстояния в терминах контрольной матрицы. Граница Гильберта-Варшамова. Коды Рида-Маллера. Коды Гоппы. NP-полнота задачи декодирования общего линейного кода по синдрому.
Р4	Циклические коды.	Связь с идеалами кольца многочленов. Коды, исправляющие пакеты ошибок. Граница Рейджера. Алгоритм исправления пакетов ошибок. Обзор кодов, исправляющих пакеты ошибок. Перемежение. Коды Файра.
Р5	Коды Боуза-ЧоудхуриХоквингема (БЧХ).	Граница БЧХ. Алгоритм Питерсона декодирования кодов БЧХ. Алгоритм Берлекэмпа. . Коды Рида-Соломона. Укороченные и каскадные коды. Алгоритм Форни.

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 кодирования

Электронные ресурсы (издания)

1. Сидельников, В. М.; Теория кодирования : учебное пособие.; Физматлит, Москва; 2008; https://biblioclub.ru/index.php?page=book&id=68384 (Электронное издание)

2. Штарьков, Ю. М.; Универсальное кодирование: Теория и алгоритмы; Физматлит, Москва; 2013; https://biblioclub.ru/index.php?page=book&id=275569 (Электронное издание)

Печатные издания

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

Профессиональные базы данных, информационно-справочные системы

Ромащенко А. Е., Румянцев А. Ю., Шень А. Р47 Заметки по теории кодирования. | М.:

МЦНМО, 2011. | 80 с. ISBN 978-5-94057-750-8 https://www.mccme.ru/~anromash/courses/coding-theory-05-2016.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 кодирования

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 Периферийное устройство Подключение к сети Интернет	Office Professional 2003 Win32 Russian CD-ROM Свободное ПО:Google Crome
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	**Не требуется**

		Рабочее место преподавателя Доска аудиторная	
5	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 псевдослучайных генераторов

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Попов Владимир Юрьевич	доктор физико-математических наук, доцент	Профессор	алгебры и фундаментальной информатики

Рекомендовано учебно-методическим советом института Естественных наук и математики

Протокол № _7_ от _21.10.2021_ г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

- **Попов Владимир Юрьевич, 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	Теория псевдослучайных генераторов на основе машин Тьюринга	Парадокс метода Монте-Карло. Понятие машины Тьюринга как псевдослучайного генератора. Применение универсальных машин Тьюринга. Применение простейших клеточных автоматов. Игра "Жизнь" как модель для порождения псевдослучайных последовательностей. Использование моделей управления при помощи глобальных сигналов для порождения псевдослучайных последовательностей. Применение Redcode для порождения псевдослучайных последовательностей. Использование эзотерических языков для порождения псевдослучайных последовательностей. Порождение псевдослучайных последовательностей на основе машины Минского. Недетерминированные машины Тьюринга для порождения псевдослучайных последовательностей.
Р2	Варианты определения случайной последовательности	Определения по Лехмеру и Франклину. Понятие краспределенности. Понятие конечной случайной последовательности.
Р3	Тесты на случайность	Алгоритм Кнута. Простейшие тесты на случайность. Chi-test. Тест Колмогорова - Смирнова. Gap test. Покерный тест. Тесты на количество значений на интервале. Перестановочные тесты. Тесты на возрастание и убывание. Распределение максимальных значений на интервале.

		Тестирование подпоследовательностей. Коэффициент корреляции. Линейные конгруэнтные последовательности. Спектральный тест. Постулаты Голомба. NIST.
Р4	Использование криптографических алгоритмов для генерации псевдослучайных чисел	Блочные алгоритмы. Потоковые шифры. Алгоритмы с открытым ключом.
Р5	Генераторы псевдослучайных последовательностей и потоковые шифры	Линейные конгруэнтные генераторы. Регистры сдвига с обратной связью. Генератор Геффе. Генератор Дженнингса. Генератор Бета-Пайпера. Пороговый генератор. Генератор Голлмана. Сжимающий генератор. Самосжимающий генератор. A5. Hughes. Nanoteq. Rambutan. Fish. Pike. Mush. M. RC4. SEAL. WAKE. Генератор Плесса.
Р6	Генераторы истинно случайных последовательностей.	Таблицы. Шум. Таймеры. Задержки. Извлеченная случайность.
Р7	Сплетения псевдослучайных генераторов	Основные свойства апериодических последовательностей с точки зрения теории псевдослучайных генераторов. Последовательность Туэ - Морса. Последовательность Фибоначчи. Механические последовательности. Методы представления информации при использовании апериодических последовательностей для генерации псевдослучайных чисел. Порождение сплетений псевдослучайных генераторов.
Р8	Интеллектуальные методы для порождения и тестирования псевдослучайных последовательностей	Нейросетевые методы. Обобщение линейных конгруэнтных генераторов на основе нейронных сетей. Применение генетических алгоритмов для порождения и тестирования псевдослучайных последовательностей.

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-исследовательск	Технология формирования уверенности и готовности к самостоятельной	ОПК-19 - Способен разрабатывать и анализировать математические модели механизмов	У-1 - Выбирать математические методы и модели для решения задач профессионально

	ая	успешной профессиональной деятельности	защиты информации	й деятельности

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Теория псевдослучайных генераторов

Электронные ресурсы (издания)

1. Гренандер, У., У., Яглом, А. М.; Случайные процессы и статистические выводы; Изд-во иностр. лит., Москва; 1961; https://biblioclub.ru/index.php?page=book&id=222424 (Электронное издание)

Печатные издания

1. Кнут, Д. Э., Козаченко, Ю. В., Красиков, И. В., Тертышный, В. Т.; Искусство программирования Т. 3. Сортировка и поиск. - 2-е изд., испр. и доп.; ВИЛЬЯМС, Москва; СПб.; Киев; 2001 (5 экз.)

2. Кнут, Д. Э., Козаченко, Ю. В., Красиков, И. В., Тертышный, В. Т.; Искусство программирования Т. 3. Сортировка и поиск. - 2-е изд., испр. и доп.; ВИЛЬЯМС, Москва; СПб.; Киев; 2000 (3 экз.)

3. Кнут, Д. Э., Козаченко, Ю. В., Красиков, И. В., Тертышный, В. Т.; Искусство программирования Т. 3. Сортировка и поиск. - 2-е изд., испр. и доп.; ВИЛЬЯМС, Москва ; СПб. ; Киев; 2003 (2 экз.)

4. Шнайер, Шнайер Б., Диффи, У., Семьянов, В. П.; Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си; Триумф, Москва; 2003 (5 экз.)

5. Шнайер, Шнайер Б., Диффи, У., Семьянов, В. П.; Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си; Триумф, Москва; 2002 (1 экз.)

Профессиональные базы данных, информационно-справочные системы

Слеповичев И.И. Генераторы псевдослучайных чисел: учебное пособие, 2017, 118с.

https://www.sgu.ru/sites/default/files/textdocsfiles/2018/07/09/slepovichev_i.i._generatory_psevdosluchaynyh_chisel_2017.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 псевдослучайных генераторов

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 Периферийное устройство Подключение к сети Интернет	Office Professional 2003 Win32 Russian CD-ROM Свободное ПО:Google Crome
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 Подключение к сети Интернет	Office Professional 2003 Win32 Russian CD-ROM Свободное ПО:Google Crome