ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Директор института
Институт естественных и точных наук

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Замышляева А. А.
Пользователь: zamyshliaevaaa
Дата подписания: 02.11.2021

А. А. Замышляева

РАБОЧАЯ ПРОГРАММА

дисциплины 1.Ф.П2.05 Математические основы криптографии
для направления 01.03.02 Прикладная математика и информатика
уровень Бакалавриат
профиль подготовки Математические методы обеспечения безопасности программных систем
форма обучения очная
кафедра-разработчик Прикладная математика и программирование

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 01.03.02 Прикладная математика и информатика, утверждённым приказом Минобрнауки от 10.01.2018 № 9

Зав.кафедрой разработчика,
д.физ.-мат.н., проф.

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Замышляева А. А.
Пользователь: zamyshliaevaaa
Дата подписания: 02.11.2021

А. А. Замышляева

Разработчик программы,
старший преподаватель (-)

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Ножкина Т. Г.
Пользователь: nozhkinatg
Дата подписания: 01.11.2021

Т. Г. Ножкина

СОГЛАСОВАНО

Руководитель образовательной программы
д.физ.-мат.н., проф.

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Замышляева А. А.
Пользователь: zamyshliaevaaa
Дата подписания: 02.11.2021

А. А. Замышляева

Челябинск

1. Цели и задачи дисциплины

Целью преподавания дисциплины "Математические основы криптографии" является изложение основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике. Задачи дисциплины - изучить основы: - системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов; - алгебраических и теоретико-числовых принципов синтеза и анализа шифров; - математических методов, используемых в криптоанализе и криптографии.

Краткое содержание дисциплины

В рамках данной дисциплины приводятся сведения из различных разделов алгебры и теории чисел, которые в дальнейшем используются в синтезе и анализе различных криптосистем.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине
ПК-6 Способен использовать математические методы при проектировании и разработке алгоритмических и программных решений в области обеспечения безопасности и защиты программных систем.	Знает: алгебраические структуры, лежащие в основе современных криптографических систем Умеет: использовать математические методы при создании криптографических спецификаций

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Нет	Ассемблер в задачах защиты информации, Математическое моделирование и прогнозирование информационных угроз, Криптографические методы защиты информации, Криптографические протоколы, Теория информации и кодирования, Квантовые коммуникации и криптография, Квантовая криптография, Программные методы защиты информации

Требования к «входным» знаниям, умениям, навыкам студента, необходимым при освоении данной дисциплины и приобретенным в результате освоения предшествующих дисциплин:

Нет

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 4 з.е., 144 ч., 74,5 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		5
Общая трудоёмкость дисциплины	144	144
Аудиторные занятия:	64	64
Лекции (Л)	32	32
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	32	32
Лабораторные работы (ЛР)	0	0
Самостоятельная работа (СРС)	69,5	69,5
с применением дистанционных образовательных технологий	0	
Подготовка к контрольным работам	39,5	39.5
Подготовка к экзамену	30	30
Консультации и промежуточная аттестация	10,5	10,5
Вид контроля (зачет, диф.зачет, экзамен)	-	экзамен

5. Содержание дисциплины

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах			
		Всего	Л	ПЗ	ЛР
1	Введение. Основные понятия алгебры. Группы, кольца, поля.	16	8	8	0
2	Поля Галуа и их основные свойства. Вычисления в полях Галуа	16	8	8	0
3	Полиномиальные функции. Построение многочлена по точкам – аппроксимационная формула Лагранжа. Кратные корни и производные	8	4	4	0
4	Линейные рекуррентные последовательности над конечным кольцом и полем	8	4	4	0
5	Эллиптические кривые	16	8	8	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1-2	1	Группы. Примеры групп. Порядок элемента в группе.	4
3	1	Кольца. Виды колец. Обратимые элементы кольца.	2
4	1	Поля. Характеристика поля.	2
5-6	2	Основная теорема о конечных полях. Алгоритм построения конечного поля.	4
7-8	2	Строение мультипликативной группы конечного поля. Дискретный логарифм и логарифм Якоби.	4
9	3	Кольцо многочленов. Неприводимость. Корни многочлена. Поле разложения.	2
10	3	Порядок многочлена и его свойства. Примитивный многочлен.	2
11-12	4	Линейные реккурентные последовательности. Минимальный период. Характеристический многочлен и ассоциированная матрица.	4

13-14	5	Определение эллиптической кривой. Классификация эллиптических кривых над различными полями. Сложение точек эллиптической кривой. Группа точек эллиптической кривой.	4
15-16	5	Криптография на эллиптических кривых. Алгоритма Полига-Хеллмана. Алгоритм Шенкса.	4

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1-2	1	Группы. Порядок элемента в группе.	4
3-4	1	Кольца. Обратимые элементы в кольцах вычетов и матричных кольцах.	4
5-6	2	Построение конечных полей.	4
7-8	2	Вычисления в конечных полях.	4
9-10	3	Неприводимость многочленов. Корни многочленов. Аппроксимационная формула Лагранжа	4
11-12	4	Линейные реккурентные последовательности над конечными полями.	4
13-14	5	Вычисления в группе точек эллиптической кривой. Порядок группы точек эллиптической кривой.	4
15-16	5	Криптография на эллиптических кривых. Алгоритма Полига-Хеллмана. Алгоритм Шенкса.	4

5.3. Лабораторные работы

Не предусмотрены

5.4. Самостоятельная работа студента

Выполнение СРС			
Подвид СРС	Список литературы (с указанием разделов, глав, страниц) / ссылка на ресурс	Семестр	Кол-во часов
Подготовка к контрольным работам	ЭУМД. осн. лит. п. 3, п. 4. ЭУМД. доп. лит. п. 1.	5	39,5
Подготовка к экзамену	ЭУМД. осн. лит. п. 3, п. 4. ЭУМД. доп. лит. п. 1.	5	30

6. Текущий контроль успеваемости, промежуточная аттестация

Контроль качества освоения образовательной программы осуществляется в соответствии с Положением о балльно-рейтинговой системе оценивания результатов учебной деятельности обучающихся.

6.1. Контрольные мероприятия (КМ)

№ КМ	Се-местр	Вид контроля	Название контрольного мероприятия	Вес	Макс. балл	Порядок начисления баллов	Учи-тыва-ется в ПА
1	5	Текущий контроль	КМ-1. Контрольная	1	10	Студенту начисляется по 1 баллу за каждую, верно решённую, задачу.	экзамен

			работа 1				
2	5	Текущий контроль	КМ-2. Контрольная работа 2	1	5	Задание 1. 1 балл - правильно построено поле; 2 балла - правильно построено поле и верно найдены все примитивные элементы; 0 баллов - в остальных случаях. Задание 2. 1 балл - задание выполнено верно, получен верный ответ; 0 баллов - в остальных случаях. Задание 3. 1 балл - задание выполнено верно, получен верный ответ; 0 баллов - в остальных случаях. Задание 4. 1 балл - задание выполнено верно, получен верный ответ; 0 баллов - в остальных случаях.	экзамен
3	5	Текущий контроль	КМ-3. Контрольная работа 3	1	8	Задание 1. Доказано, что уравнение задаёт эллиптическую кривую - 1 балл. Верно найдена группа точек эллиптической кривой - 1 балл. Верно найдена сумма точек в п. а) - 1 балл. Верно найдена сумма точек в п. б) - 1 балл. Задание 2. Верно найден порядок группы точек эллиптической кривой - 1 балл. Верно найдена группа точек эллиптической кривой над первым полем - 1 балл. Верно найдена группа точек эллиптической кривой над вторым полем - 1 балл. Задание 3. 1 балл - задание выполнено верно, получен верный ответ. 0 баллов - в остальных случаях.	экзамен
4	5	Текущий контроль	КМ-4. Активная познавательная деятельность	1	64	На каждом из 32 занятий студент может получить 2 балла: Студент задает вопросы по изучаемому материалу - 1 балл; Студент правильно отвечает на вопросы по изучаемому материалу - 1 балл. В противном случае баллы не начисляются.	экзамен
5	5	Проме-жуточная аттестация	КМ-5. Экзамен	1	10	Теоретический вопрос 1. 2 балла - студент дал верный полный ответ на вопрос. 1 балл - студент дал верный ответ на вопрос, но не полный. 0 баллов - ответ не верный или нет ответа.	экзамен

						Теоретический вопрос 2. 2 балла - студент дал верный полный ответ на вопрос. 1 балл - студент дал верный ответ на вопрос, но не полный. 0 баллов - ответ не верный или нет ответа. Практическое задание 1. 2 балла - студент верно решил задачу, получен верный ответ. 1 балл - студент верно решил задачу, но ответ получен не верный из-за одной-двух вычислительных ошибок. 0 баллов - в остальных случаях. Практическое задание 2. 2 балла - студент верно решил задачу, получен верный ответ. 1 балл - студент верно решил задачу, но ответ получен не верный из-за одной-двух вычислительных ошибок. 0 баллов - в остальных случаях. Практическое задание 3. 2 балла - студент верно решил задачу, получен верный ответ. 1 балл - студент верно решил задачу, но ответ получен не верный из-за одной-двух вычислительных ошибок. 0 баллов - в остальных случаях.	

6.2. Процедура проведения, критерии оценивания

Вид промежуточной аттестации	Процедура проведения	Критерии оценивания
экзамен	Рейтинг обучающегося по дисциплине формируется по результатам текущего контроля и контрольного мероприятия промежуточной аттестации, которое является обязательным. Контрольное мероприятие экзамена проводится в очной форме. Студенту выдаётся билет. Даётся 90 минут для подготовки к ответу. Проводится собеседование по выданным вопросам.	В соответствии с пп. 2.5, 2.6 Положения

6.3. Оценочные материалы

Компетенции	Результаты обучения	№ КМ				
		1	2	3	4	5
ПК-6	Знает: алгебраические структуры, лежащие в основе современных криптографических систем	+	+	+	+	+
ПК-6	Умеет: использовать математические методы при создании криптографических спецификаций				+	+

Фонды оценочных средств по каждому контрольному мероприятию находятся в приложениях.

7. Учебно-методическое и информационное обеспечение дисциплины

Печатная учебно-методическая документация

а) основная литература:

Не предусмотрена

б) дополнительная литература:

Не предусмотрена

в) отечественные и зарубежные журналы по дисциплине, имеющиеся в библиотеке:

Не предусмотрены

г) методические указания для студентов по освоению дисциплины:

1. Зюляркина Н. Д. Криптографические методы защиты информации. Методические указания по проведению практических занятий

из них: учебно-методическое обеспечение самостоятельной работы студента:

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание
1	Дополнительная литература	Электронно-библиотечная система издательства Лань	Рябко, Б. Я. Основы современной криптографии и стеганографии : монография / Б. Я. Рябко, А. Н. Фионов. — 2-е изд. — Москва : Горячая линия-Телеком, 2016. — 232 с. — ISBN 978-5-9912-0350-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111098 (дата обращения: 01.11.2021). — Режим доступа: для авториз. пользователей.
2	Дополнительная литература	Электронно-библиотечная система издательства Лань	Глухов, М. М. Элементы теории обыкновенных представлений и характеров конечных групп с приложениями в криптографии : учебное пособие / М. М. Глухов, И. А. Круглов. — Санкт-Петербург : Лань, 2015. — 176 с. — ISBN 978-5-8114-1855-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/65044 (дата обращения: 01.11.2021). — Режим доступа: для авториз. пользователей.
3	Основная литература	Электронно-библиотечная система издательства Лань	Введение в теоретико-числовые методы криптографии : учебное пособие / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. — Санкт-Петербург : Лань, 2021. — 400 с. — ISBN 978-5-8114-1116-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/167921 (дата обращения: 01.11.2021). — Режим доступа: для авториз. пользователей.
4	Основная литература	Электронно-библиотечная система издательства Лань	Пилиди, В. С. Математические основы защиты информации : учебное пособие / В. С. Пилиди. — Ростов-на-Дону : ЮФУ, 2019. — 308 с. — ISBN 978-5-9275-3363-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/141130 (дата обращения: 01.11.2021). — Режим доступа: для авториз. пользователей.

Перечень используемого программного обеспечения:

Нет

Перечень используемых профессиональных баз данных и информационных справочных систем:

Нет

8. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
Лекции	330 (3б)	Доска, мел.
Практические занятия и семинары	330 (3б)	Доска, мел.