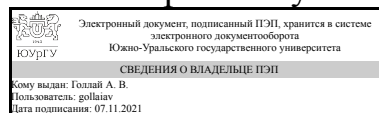


ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Директор института
Высшая школа электроники и
компьютерных наук



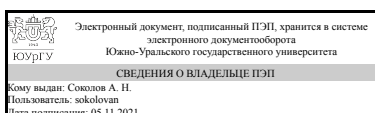
А. В. Голлай

РАБОЧАЯ ПРОГРАММА

**дисциплины Б.1.29 Математические основы криптологии
для направления 10.03.01 Информационная безопасность
уровень бакалавр тип программы Бакалавриат
профиль подготовки Безопасность автоматизированных систем
форма обучения очная
кафедра-разработчик Защита информации**

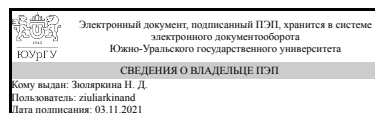
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность, утверждённым приказом Минобрнауки от 01.12.2016 № 1515

Зав.кафедрой разработчика,
к.техн.н., доц.



А. Н. Соколов

Разработчик программы,
д.физ.-мат.н., доц., профессор



Н. Д. Зюляркина

1. Цели и задачи дисциплины

Дисциплина "Математические основы криптологии" обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом, содействует формированию мировоззрения и системного мышления. Целью преподавания дисциплины "Математические основы криптологии" является изложение основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике. Задачи дисциплины - дать 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 (ЗУНы)
ПК-9 способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	Знать:основные алгебраические и теоретико-числовые методы, применяемые в криптографии
	Уметь:подбирать научную литературу, посвященную алгебраическим методам в криптографии
	Владеть:криптографической терминологией
ПК-2 способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Знать:характеристики программных разработок, позволяющих работать с алгебраическими структурами.
	Уметь:производить вычисления с помощью пакета GAP и аналогичных программных комплексов
	Владеть:навыками программирования в пакете GAP
ОПК-2 способностью применять соответствующий математический аппарат для решения профессиональных задач	Знать:определения и свойства основных алгебраических структур: групп, колец и полей.
	Уметь:производить вычисления в кольцах вычетов, матричных кольцах и в конечных полях
	Владеть:навыками работы с элементами групп, колец и полей

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Б.1.06.01 Алгебра и геометрия	Б.1.22 Криптографические методы защиты

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

Дисциплина	Требования
Б.1.06.01 Алгебра и геометрия	знать: основные алгебраические структуры: группы, кольца, поля

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 3 з.е., 108 ч.

Вид учебной работы	Всего часов	Распределение по семестрам в часах	
		Номер семестра	
		6	
Общая трудоёмкость дисциплины	108	108	
<i>Аудиторные занятия:</i>	48	48	
Лекции (Л)	32	32	
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	16	16	
Лабораторные работы (ЛР)	0	0	
<i>Самостоятельная работа (СРС)</i>	60	60	
Подготовка к практическим занятиям	40	40	
Написание программ, реализующих алгебраические и теоретико-числовые алгоритмы	20	20	
Вид итогового контроля (зачет, диф.зачет, экзамен)	-	зачет	

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.	12	8	4	0
2	Алгебраические методы в криптологии. Поля Галуа и их основные свойства. Вычисления в полях Галуа	12	8	4	0
3	Полиномиальные функции. Построение многочлена по точкам – аппроксимационная формула Лагранжа. Кратные корни и производные	6	4	2	0
4	Линейные рекуррентные последовательности над конечным кольцом и полем	8	6	2	0
5	Эллиптические кривые	10	6	4	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во
----------	-----------	---	--------

			часов
1	1	Группы. Примеры групп. Порядок элемента в группе.	4
3	1	Поля. Характеристика поля.	2
4	1	Кольца. Виды колец. Обратимые элементы кольца	2
4	2	Основная теорема о конечных полях. Алгоритм построения конечного поля.	4
5	2	Строение мультипликативной группы конечного поля. Дискретный логарифм и логарифм Якоби.	4
6	3	Кольцо многочленов. Неприводимость. Корни многочлена. Поле разложения.	2
7	3	Порядок многочлена и его свойства. Примитивный многочлен.	2
8	4	Линейные рекуррентные последовательности. Минимальный период. Характеристический многочлен и ассоциированная матрица.	6
9	5	Определение эллиптической кривой. Классификация эллиптических кривых над различными полями. Сложение точек эллиптической кривой. Группа точек эллиптической кривой	6

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	1	Группы. Порядок элемента в группе. Кольца. Обратимые элементы в кольцах вычетов и матричных кольцах.	3
2	1	Контрольная работа по теме "Алгебраические структуры"	1
3	2	Построение конечного поля. Вычисления в конечных полях	2
4	2	Контрольная работа по теме "Поля"	2
5	3	Неприводимость многочленов. Корни многочленов	1
6	3	Контрольная работа по теме "Многочлены над конечными полями"	1
7	4	Линейные рекуррентные последовательности над конечными полями.	2
8,9	5	Вычисления в группе точек эллиптической кривой. Порядок группы точек эллиптической кривой.	3
10	5	Контрольная работа по теме "Эллиптические кривые"	1

5.3. Лабораторные работы

Не предусмотрены

5.4. Самостоятельная работа студента

Выполнение СРС		
Вид работы и содержание задания	Список литературы (с указанием разделов, глав, страниц)	Кол-во часов
Написание программ, реализующих алгебраические и теоретико-числовые алгоритмы	Основная печатная литература: п3 (разделы 1-4).	20
Подготовка к практическим занятиям	Основная печатная литература: п1 (Глава 1), п.2 (Глава 1).	40

6. Инновационные образовательные технологии, используемые в учебном процессе

Инновационные формы учебных занятий	Вид работы	Краткое	Кол-во ауд.
-------------------------------------	------------	---------	-------------

	(Л, ПЗ, ЛР)	описание	часов
не предусмотрены	Лабораторные занятия		0

Собственные инновационные способы и методы, используемые в образовательном процессе

Инновационные формы обучения	Краткое описание и примеры использования в темах и разделах
не предусмотрены	не предусмотрены

Использование результатов научных исследований, проводимых университетом, в рамках данной дисциплины: нет

7. Фонд оценочных средств (ФОС) для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

7.1. Паспорт фонда оценочных средств

Наименование разделов дисциплины	Контролируемая компетенция ЗУНы	Вид контроля (включая текущий)	№№ заданий
Введение. Основные понятия алгебры. Группы, кольца, поля.	ОПК-2 способностью применять соответствующий математический аппарат для решения профессиональных задач	Домашние задания. Контрольная работа	1
Алгебраические методы в криптологии. Поля Галуа и их основные свойства. Вычисления в полях Галуа	ОПК-2 способностью применять соответствующий математический аппарат для решения профессиональных задач	Домашние задания. Контрольная работа	2
Эллиптические кривые	ОПК-2 способностью применять соответствующий математический аппарат для решения профессиональных задач	Домашние задания. Контрольная работа	3
Все разделы	ПК-2 способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Написание программы в пакете GAP	4
Все разделы	ПК-9 способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	Подготовка реферата и доклад.	5
Все разделы	ОПК-2 способностью применять соответствующий математический аппарат для решения профессиональных задач	Зачёт	6

7.2. Виды контроля, процедуры проведения, критерии оценивания

Вид	Процедуры проведения и оценивания	Критерии оценивания
-----	-----------------------------------	---------------------

контроля		
	проверка приведенных решений	Отлично: все задания решены верно Хорошо: около 3/4 заданий решено верно, есть незначительные ошибки Удовлетворительно: не менее половины заданий решено верно, но присутствуют существенные ошибки Неудовлетворительно: решено менее половины заданий
	проверка реферата и прослушивание доклада	Зачтено: тема доклада раскрыта Не зачтено: тема доклада не раскрыта
		Зачтено: программа при тестировании выдает правильный результат Не зачтено: программа не работает или выдает неверный результат
	Зачет проводится в форме устного опроса. В аудитории, где проводится зачет, должно одновременно присутствовать не более 6-8 студентов. Каждому студенту задается по одному вопросу или заданию из каждой темы, выносимой на зачет. При неправильном ответе студенту могут быть заданы уточняющие или новые вопросы из этой темы. Т	Зачтено: Выполнено хотя бы одно задание билета без замечаний. Зачтены все контрольные работы. Не зачтено: Выполнено менее одного задания билета или имеются значительные замечания. Имеются незачтенные контрольные работы.

7.3. Типовые контрольные задания

Вид контроля	Типовые контрольные задания
	методкрипто33.doc
	темы тодкладов по мок.docx
	программы по МОК.docx
	<ol style="list-style-type: none"> 1. Определение группы, кольца, поля. 2. Порядок элемента в группе. 3. Основная теорема о конечных полях. 4. Характеристика поля. Число элементов поля. 5. Расширение поля. 6. Примитивный элемент поля. 7. Логарифм Якоби для записи элементов конечного поля 8. Построение многочлена по точкам - аппроксимационная формула Лагранжа. 9. Кратные корни и производные. 10. Расширение поля через присоединение корней. 11. Линейные рекуррентные последовательности. 12. Эллиптические кривые 13. Эллиптическая кривая над конечным полем. 14. Сложение точек на эллиптической кривой.

8. Учебно-методическое и информационное обеспечение дисциплины

Печатная учебно-методическая документация

а) основная литература:

Не предусмотрена

б) дополнительная литература:

1. Ван-дер-Варден, Б. Л. Алгебра Б. Л. ван дер Варден; Пер. с нем. А. А. Бельский. - 3-е изд., стер. - СПб.: Лань, 2004. - 623 с.

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	Основная литература	Электронно-библиотечная система издательства Лань	Глухов, М.М. Введение в теоретико-числовые методы криптографии. [Электронный ресурс] / М.М. Глухов, И.А. Круглов, А.Б. Пичкур, А.В. Черемушкин. — Электрон. дан. — СПб. : Лань, 2011. — 400 с. — Режим доступа: http://e.lanbook.com/book/68466 — Загл. с экрана.
2	Дополнительная литература	Электронно-библиотечная система издательства Лань	Глухов, М.М. Элементы теории обыкновенных представлений и характеров конечных групп с приложениями в криптографии. [Электронный ресурс] / М.М. Глухов, И.А. Круглов. — Электрон. дан. — СПб. : Лань, 2015. — 176 с. — Режим доступа: http://e.lanbook.com/book/65044 — Загл. с экрана.

9. Информационные технологии, используемые при осуществлении образовательного процесса

Перечень используемого программного обеспечения:

Нет

Перечень используемых информационных справочных систем:

Нет

10. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
-------------	--------	--

Лекции	912 (36)	Комплект компьютерного оборудования, LCD Проектор, Экран проекционный, настенные стенды по защите информации (5 шт.), программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozila Firefox, Консультант+.
Практические занятия и семинары	913 (36)	Комплект компьютерного оборудования; Локальная вычислительная сеть; Коммутатор, Программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozila Firefox, Консультант+; Локальные СЗИ: Secret Net 6.5 (автономный вариант), Страж 3.0; Межсетевые экраны: ViPNet Custom 3.1, User Gate 5.2