МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
Факультет информационных систем и безопасности
Кафедра фундаментальной и прикладной математики

КОНЕЧНЫЕ ПОЛЯ И ИХ ПРИЛОЖЕНИЯ К КРИПТОГРАФИИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Направление подготовки 01.03.04 Прикладная математика
Направленность (профиль) Математика информационных сред

Уровень высшего образования: бакалавриат
Форма обучения: очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2022

КОНЕЧНЫЕ ПОЛЯ И ИХ ПРИЛОЖЕНИЯ К КРИПТОГРАФИИ
Рабочая программа дисциплины

Составители:
Д. пед. н., профессор, профессор кафедры фундаментальной и прикладной математики
В.К. Жаров
Д. ф.-м. н., профессор, профессор кафедры фундаментальной и прикладной математики
В.М. Максимов

УТВЕРЖДЕНО
Протокол заседания кафедры
фундаментальной и прикладной математики
№ 10 от 05.04.2022

ОГЛАВЛЕНИЕ

1.# Пояснительная записка ..... 4#
1.1.# Цель и задачи дисциплины ..... 4#
1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций ..... 4#
1.3. Место дисциплины в структуре образовательной программы ..... 5#
2.# Структура дисциплины ..... 5#
3.# Содержание дисциплины ..... 5#
4.# Образовательные технологии ..... 6#
5.# Оценка планируемых результатов обучения ..... 6#
5.1# Система оценивания ..... 6#
5.2# Критерии выставления оценки по дисциплине ..... 6#
5.3# Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине ..... 7#
6.# Учебно-методическое и информационное обеспечение дисциплины ..... 9#
6.1# Список источников и литературы ..... 9#
6.2# Перечень ресурсов информационно-телекоммуникационной сети «Интернет». ..... 10#
6.3# Профессиональные базы данных и информационно-справочные системы ..... 10#
7.# Материально-техническое обеспечение дисциплины ..... 10#
8.# Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов ..... 10#
9.# Методические материалы ..... 11#
9.1# Планы практических занятий ..... 11#
9.2# Методические рекомендации по подготовке письменных работ ..... 13#
Приложение 1. Аннотация рабочей программы дисциплины ..... 14#

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины: показать теорию и задачи, решаемые с её помощью имеющие богатое практическое применение в реальной практике работы в экономической сфере, технике и в задачах защиты информации.
Задачи дисциплины: в результате изучения дисциплины студенты должны владеть основными математическими понятиями курса; уметь решать типовые задачи, иметь навыки работы со специальной математической литературой, уметь использовать математический аппарат для решения теоретических и прикладных задач.

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
ПК-2. Способен выделять, формулировать возникающие в результате самостоятельной научной деятельности или деятельности научных, производственных, административных учреждений задачи или подзадачи для решения текущих проблем	ПК-2.1. Владеет навыками работы с информационными системами	***Знать**:* основные теоремы теории чисел, используемые в криптологии; основные теоретико-числовые алгоритмы; ***Уметь***: программно реализовывать основные теоретико-числовые и получисленные алгоритмы в криптографических приложениях; выполнять построение криптосистем на основе готовых криптографических библиотек; ***Владеть:*** навыками работы с алгоритмами криптоанализа ассиметричных криптосистем.
	ПК-2.2. Рассматривает социотехнические системы как совокупность информационных систем	***Знать**:* основные теоретико-числовые алгоритмы; основные алгоритмы, реализующие арифметические операции в основных алгебраических структурах, используемых в криптографических приложениях; ***Уметь***: выполнять построение криптосистем на основе готовых криптографических библиотек; проводить математическое моделирование в криптологии; приводить математическое доказательство работоспособности предложенной криптосистемы; ***Владеть:*** навыками работы с алгоритмами криптоанализа ассиметричных криптосистем.
	ПК-2.3. В совершенстве владеет методами передачи информации и применения пакетов прикладных программ	***Знать**:* основные алгоритмы, реализующие арифметические операции в основных алгебраических структурах, используемых в криптографических приложениях; ***Уметь***: проводить математическое моделирование в криптологии; приводить математическое доказательство работоспособности

		предложенной криптосистемы; ***Владеть:*** навыками работы с алгоритмами криптоанализа ассиметричных криптосистем.

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Конечные поля и их приложения к криптографии» относится к части, формируемой участниками образовательных отношений части блока дисциплин учебного плана.
Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин (модулей): «Математический анализ», «Общая алгебра и теория чисел», «Функциональный анализ».
В результате освоения дисциплины формируются знания, умения и владения, необходимые для прохождения Производственной практики (Научно-исследовательская работа) и написания выпускной квалификационной работы.

2. Структура дисциплины

Общая трудоёмкость дисциплины составляет 4 з.е., 144 академических часа.

Структура дисциплины для очной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
8	Лекции	**24**
8	Практические занятия	**32**
	Всего:	**56**

Объем дисциплины в форме самостоятельной работы обучающихся составляет 88 академических часов.

3. Содержание дисциплины

Тема 1. Определение колец и полей. Кольца без делителей нуля. Основные понятия. Идеалы, Фактор кольца: свойства.
Тема 2. Конечные поля и кольца. Характеристика поля и кольца. Простые поля. Характеристики поля и кольца. Кольца частных. Числовые поля.
Тема 3. Число элементов конечного поля. Поле вычетов по модулю p. Поле p-адических чисел. Примеры нечисловых полей. Символические присоединения. Конечные поля (приложения).
Тема 4. Кольцо многочленов из данного конечного поля. Теорема Безу. Неприводимые многочленов.
Нормирование алгебраических полей: общий случай. Нормирование полей алгебраических чисел. Теорема Островского.
Тема 5. Простое алгебраическое расширение конечного поля.
Арифметические операции в Q_p. p-адические разложения рациональных чисел. Лемма Гензеля.
Тема 6. Поля разложение данного многочлена над конечным полем Теорема существования. Теорема о разложение над универсальным полем.
Тема 7. Теорема о существования конечного поля числом элементов p .
Тема 8. Применение конечных полей в криптоалгоритмах. Примеры p-адических шифров.

4. Образовательные технологии

Для проведения *занятий лекционного типа* по дисциплине применяются такие образовательные технологии как проблемная лекция.
Для проведения *практических занятий* используются такие образовательные технологии как: решение типовых задач для закрепления и формирования знаний, умений, навыков.
В рамках *самостоятельной работы* студентов проводится консультирование и проверка домашних заданий посредством электронной почты.

В период временного приостановления посещения обучающимися помещений и территории РГГУ для организации учебного процесса с применением электронного обучения и дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:

– видео-лекции**;**
– онлайн-лекции в режиме реального времени;
– электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;
– системы для электронного тестирования;
– консультации с использованием телекоммуникационных средств.

5. Оценка планируемых результатов обучения

5.1 Система оценивания

Форма контроля	Макс. количество баллов	
	За одну работу	Всего
Текущий контроль: - опрос, доклад, реферат - РГР, защита РГР - коллоквиум	 6 баллов 20 баллов 10 баллов	 30 баллов 20 баллов 10 баллов
Промежуточная аттестация - экзамен (Экзамен по билетам)		40 баллов
Итого за семестр		100 баллов

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2 Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
100-83/ A,B	отлично	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	хорошо	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D,E	удовлетво-рительно	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	неудовлет-ворительно	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

5.3 Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

Текущий контроль

Примерные темы рефератов, докладов

1. Символическое присоединение
2. Поля разложения
3. Расширения числовых полей

4. Определение поля p-адических чисел
5. Поля Галуа
6. Норма p-адического числа
7. Арифметические операции в Q_p
8. p-адическое продолжение рациональных чисел
9. Лемма Гензеля
10. Метрика и норма для рациональных чисел. Теорема Островского
11. Последовательности и ряды p-адических чисел
12. p-адические функции
13. Дифференцирование p-адических функций
14. Интегрирование p-адических функций

Примерные вопросы для коллоквиума

1. Построение поля действительных чисел.
2. Нормированные поля.
3. Пополнение нормированного поля.
4. Поле p-адических чисел.
5. p-адическое разложение рациональных чисел.
6. Алгебраические свойства целых p-адических чисел.
7. Метрики и нормы на поле p-адических чисел.
8. Теорема Островского.
9. Элементарные функции, определенные на поле p-адических чисел.
10. Нули p-адических степенных рядов
11. Свойства p-адических экспонент и логарифмов.
12. Локально постоянные функции.
13. Дифференцируемость p-адических чисел.

Примерные задания для РГР

1. Верно ли, что мультипликативная группа F_q^* поля F_q - циклическая группа порядка $q-1$.
2. Всякий полином $f(x) \in F_p[x]$ степени m является делителем полинома $x^{p^{mc}} - x$ для произвольного натурального $\boldsymbol{c}$.
3. Множество полином $p(x) \in F_p[x]$ делящих полином $x^{p^m} - x$, представляет совокупность всех неприводимых полиномов степени n для всех делителей n чисел m.
4. Пусть $\varphi : F_q \to F_q$ **произвольное** отображение поля F_q в себя. Покажите, что функция $\varphi(x)$ может быть представлена полиномом с коэффициентами из F_q степени не большей, чем $q-1$.

Промежуточная аттестация

Примерные контрольные вопросы по курсу

1. Нормированные поля.
2. Пополнение нормированного поля.
3. Поле p-адических чисел.
4. p-Адическое разложение рациональных чисел.
5. Алгебраические свойства целых p-адических чисел.
6. Метрики и нормы на поле p-адических чисел.
7. Теорема Островского.
8. Элементарные функции, определенные на поле p-адических чисел.
9. Нули p-адических степенных рядов
10. Свойства p-адических экспонент и логарифмов.
11. Локально постоянные функции.
12. Дифференцируемость p-адических чисел.

Примерные практические задания

1) Для каждого из следующих чисел n = 19, 27, 60 найти в кольце Z/n
Все делители нуля, все единицы и обратные к ним элементы.

2) Пусть $f(X) = X^2 - 2 \in Z[X]$. Для каждого из простых чисел p = 2,3,7 установить, существует или нет корень f(X) :

a) mod p, b) mod p^2, c) mod p^3, d) mod p^4 .

3) Найти генератор циклической группы единиц $(Z/n)^\times$ в каждом из следующих колец:

a) Z/23, b) Z/27, c) Z/10.

4) Используя лемму Гензеля решить уравнения:

a) $X^2 + 6 \underset{625}{\equiv} 0$ b) $X^2 + X + 8 \underset{2401}{\equiv} 0$

5) Пусть p простое число, $x \in Q$, Рассмотрим последовательность e_n , где $e_n = \sum_{0 \le i \le n} \frac{x^i}{i!}$. Показать, что последовательность e_n является фундаментальной относительно нормы $|\ |_p$, если (a) $|x_p|<1$, или (b) p=2 и $|x|_2<1/2$.

6) Дан p-адический степенной ряд $\sum_{n=1}^{\infty} p^{-n} x^n$ найти множество сходимости ряда и нули его суммы.

7) Функция f: $Z_p \to Z_p$ определена равенством $f\left(\sum_{n=0}^{\infty} a_n p^n\right) = \sum_{n=0}^{\infty} a_n^2 p^n$. Доказать непрерывность f.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Список источников и литературы

Литература

Основная

1. Коблиц Нил. Курс теории чисел и криптографии / Н. Коблиц; [пер. с англ. М. А. Михайловой и В. Е. Тараканова под ред. А. М. Зубкова]. - М.: ТВП, 2001. - X, 260 с.

Дополнительная

1.Рудин Уолтер. Основы математического анализа / Уолтер Рудин; Пер. с англ. В.П. Хавина. - Изд. 3-е, стер. - СПб. : Лань, 2002. - 319 с.
2.Кириллов А.А. Что такое число?. - М.: Наука, 1993. - 78с.

6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

Единое окно доступа к образовательным ресурсам - http://window.edu.ru/window/library
Дифференциальное исчисление - http://math.ru/lib/3

Национальная электронная библиотека (НЭБ) www.rusneb.ru
ELibrary.ru Научная электронная библиотека www.elibrary.ru

6.3 Профессиональные базы данных и информационно-справочные системы

Доступ к профессиональным базам данных: https://liber.rsuh.ru/ru/bases

Информационные справочные системы:
1. Консультант Плюс
2. Гарант

7. Материально-техническое обеспечение дисциплины

Для обеспечения дисциплины используется материально-техническая база образовательного учреждения: учебные аудитории, оснащённые доской, компьютером или ноутбуком, проектором (стационарным или переносным) для демонстрации учебных материалов.

Состав программного обеспечения:
1. Windows
2. Microsoft Office
3. Kaspersky Endpoint Security

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением или могут быть заменены устным ответом; обеспечивается индивидуальное равномерное освещение не менее 300 люкс; для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств; письменные задания оформляются увеличенным шрифтом; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.
- для глухих и слабослышащих: лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования; письменные задания выполняются на компьютере в письменной форме; экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

- для лиц с нарушениями опорно-двигательного аппарата: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих: в печатной форме увеличенным шрифтом, в форме электронного документа, в форме аудиофайла.
- для глухих и слабослышащих: в печатной форме, в форме электронного документа.
- для обучающихся с нарушениями опорно-двигательного аппарата: в печатной форме, в форме электронного документа, в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих: устройством для сканирования и чтения с камерой SARA CE; дисплеем Брайля PAC Mate 20; принтером Брайля EmBraille ViewPlus;
- для глухих и слабослышащих: автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих; акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата: передвижными, регулируемыми эргономическими партами СИ-1; компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1 Планы практических занятий

Тема 1. Конечные поля и кольца. Характеристика поля и кольца.

Цель занятия: Основные понятия конечных полей и колец.

Форма проведения – решение типовых задач для закрепления и формирования знаний, умений, навыков.

Задания:

1. Докажите, что число рационально тогда и только тогда, когда пред¬ставляющая его бесконечная десятичная дробь является периодической.
2. Докажите, что для любой последовательности Коши рациональных чисел относительно евклидова расстояния существует эквивалентная ей последовательность частичных сумм ряда вида (1.2).
3. Используя представление действительных чисел в виде бесконечных десятичных дробей, докажите, что множество действительных чисел пол¬но относительно евклидова

расстояния, т. е. что любая последовательность Коши, состоящая из действительных чисел, имеет предел.

5. Докажите, что следующие метрические пространства не являются полными, и постройте их пополнения:

A с расстоянием d(x, y) = |arctgx - arctgy|;

R с расстоянием d(x, y) = \ex - ey\.

6. Докажите, что метрическое пространство полно тогда и только то¬гда, когда любая

последовательность вложенных замкнутых шаров {Bп}, B] D B2 D B3 D ..., радиусы которых стремятся к нулю, имеет единствен¬ную общую точку.

Контрольные вопросы:

Построение поля действительных чисел.

Нормированные поля.

Тема 2. Число элементов конечного поля. Поле вычетов по модулю p.

Цель занятия: Поле вычетов по модулю p.

Форма проведения – решение типовых задач для закрепления и формирования знаний, умений, навыков.

Задания:

1. Целые числа 2, 3, 4 обратимы в Z5. Найдите 5-адические разло¬жения обратных к ним.

2. Найдите разложение числа 1/3 в Zm.

3. Найдите 4 цифры канонических разложений следующих p-адиче¬ских чисел:

1) …1211 в Q7; 1 : ... 1323 в Z5;

2) 900 - ...312,3 в Q11;

Контрольные вопросы:

Поле p-адических чисел.

p-адическое разложение рациональных чисел.

Алгебраические свойства целых p-адических чисел.

Метрики и нормы на поле p-адических чисел, приведите примеры.

Тема 3. Простое алгебраическое расширение конечного поля.

Цель занятия: основные понятия предваряющие понятие алгебраическое расширение, в том числе и само это определение, примеры алгебраических расширений.

Форма проведения – решение типовых задач для закрепления и формирования знаний, умений, навыков.

Задания:

1. Докажите, что если число g составное, то функция является псевдонормой, т.е. она удовлетворяет свойствам

1) и 3) из определения 2.1, а также неравенству (10.1).

2. Докажите, что Q10 не является полем, предъявив делители нуля.

3. Рассмотрим следующую последовательность натуральных чисел: 6, 76, 376, 9376, 109376...

Докажите, что эту последовательность можно продолжить одно¬значно таким образом, чтобы получить 10-адическое число a = ... 109376, удовлетворяющее уравнению a2 = a.

4. Докажите, что уравнение x2 = x имеет в Z10 четыре корня, а именно 0, 1, a и ß. Найдите первые 6 цифр числа ß.

5. Докажите, что Z10 (прямое произведение групп).

Контрольные вопросы:

Метрики и нормы на поле p-адических чисел.

Теорема Островского.

Элементарные функции, определенные на поле p-адических чисел.

Тема 4. Поля разложение данного многочлена над конечным полем. Теорема существования.

Цель занятия: методы разложения многочлена над конечным полем

Форма проведения – решение типовых задач для закрепления и формирования знаний, умений, навыков.

Задания:

1.Докажите, что отображение непрерывно тогда и только тогда, когда оно непрерывно в каждой точке.

2. Докажите, что непрерывный образ связного множества связан.

3. Верно ли, что если — монотонное взаимно однозначное отображение двух замкнутых подмножеств W. Тогда — гомеомор¬физм.

Контрольные вопросы:

Теорема Островского.

Элементарные функции, определенные на поле р-адических чисел.

Нули р-адических степенных рядов

Свойства р-адических экспонент и логарифмов.

Локально постоянные функции.

Дифференцируемость р-адических чисел.

9.2 Методические рекомендации по подготовке письменных работ

Требования к подготовке и содержанию письменных работ (реферата, доклада):

1. Соответствие содержания теме и плану работы.
2. Полнота и глубина раскрытия основных понятий проблемы.
3. Достаточность фактов, позволяющих проиллюстрировать актуальность избранной проблемы, способы ее решения.
4. Работа с литературой, систематизация и структурирование материала.
5. Обобщение и сопоставление различных точек зрения по рассматриваемому вопросу.
6. Наличие и четкость выводов, резюме.

Приложение 1. Аннотация
рабочей программы дисциплины

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Дисциплина «Конечные поля и их приложения к криптографии» реализуется на факультете информационных систем и безопасности кафедрой фундаментальной и прикладной математики.

Цель дисциплины: показать теорию и задачи, решаемые с её помощью имеющие богатое практическое применение в реальной практике работы в экономической сфере, технике и в задачах защиты информации.

Задачи дисциплины: в результате изучения дисциплины студенты должны владеть основными математическими понятиями курса; уметь решать типовые задачи, иметь навыки работы со специальной математической литературой, уметь использовать математический аппарат для решения теоретических и прикладных задач.

Дисциплина направлена на формирование следующих компетенций:

ПК-2. Способен выделять, формулировать возникающие в результате самостоятельной научной деятельности или деятельности научных, производственных, административных учреждений задачи или подзадачи для решения текущих проблем.

Знать: основные теоремы теории чисел, используемые в криптологии; основные теоретико-числовые алгоритмы; основные алгоритмы, реализующие арифметические операции в основных алгебраических структурах, используемых в криптографических приложениях;

Уметь: программно реализовывать основные теоретико-числовые и получисленные алгоритмы в криптографических приложениях; выполнять построение криптосистем на основе готовых криптографических библиотек; проводить математическое моделирование в криптологии; приводить математическое доказательство работоспособности предложенной криптосистемы;

Владеть: навыками работы с алгоритмами криптоанализа ассиметричных криптосистем.

По дисциплине предусмотрена промежуточная аттестация в форме экзамена.

Общая трудоемкость освоения дисциплины составляет 4 зачетные единицы.