Программа учебной дисциплины
маголего «Математические основы защиты информации»

Утверждена
Проректором С.Ю.Рощиным
«25» июня 2018 г.

Автор	И.В.Артамкин, д.ф-м.н., профессор
Число кредитов	3
Контактная работа (час.)	32
Самостоятельная работа (час.)	82
Курс	1
Формат изучения дисциплины	Без использования онлайн курса

I. ЦЕЛЬ, РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ И ПРЕРЕКВИЗИТЫ

Целями освоения дисциплины «Математические основы защиты информации» является

- Формирование у слушателей ясного представления об основных алгебраических структурах, используемых в современной криптографии;
- Знакомство с использованием конечных полей для генерации периодических последовательностей;
- Углублённое изучение структуры конечных полей и умение проводить в них явные вычисления.

В результате освоения дисциплины студент должен:

знать:

- общее представление о применении современной алгебры в криптографии;
- Изучить основные понятия и простейшие результаты теории групп, колец и полей;

уметь:

- проводить явные вычисления в конечных полях;

иметь навыки:

- Углублённого изучение структуры конечных полей и умения проводить в них явные вычисления.

Изучение дисциплины «Математические основы защиты информации базируется на хорошем владении школьным курсом математики и основными понятиями базового курса линейной алгебры.

Основные положения дисциплины должны быть использованы в дальнейшем при изучении более продвинутых курсов алгебры и прикладных курсов по защите информации, криптографии и теории кодирования.

II. СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Тема 1. Диофантовы уравнения. Алгоритм Евклида.
Тема 2. Кольца вычетов. Простейшие свойства

Тема 3. Простейшие алгебраические структуры: группы, кольца, поля.

Тема 4. Китайская теорема об остатках. Теоремы Эйлера и Ферма. Функция Эйлера.

Тема 5. Кольцо многочленов.

Тема 6: Построение фактор-кольца многочленов и вычисления в них.

Тема 7. Фактор-кольца кольца многочленов и сдвиговый регистр

Тема 8. Конечные поля и генерация периодических последовательностей

Тема 9. Строение конечных полей.

III. ОЦЕНИВАНИЕ

Итоговая оценка по курсу совпадает с накопленной; экзамен не предусмотрен. Накопленная оценка складывается из оценок за пятиминутные аудиторные проверочные работы (30%) и индивидуального письменного домашнего задания (70%), или же из решения задач повышенной сложности. Задачи подбираются так, чтобы их решение потребовало от студента свободного владения основными понятиями и умения пользоваться техническими (вычислительными) приемами, которые изучаются в соответствующем разделе курса. Часть задач повышенной сложности носят исследовательский характер и предполагают самостоятельное изучение студентами материала, не излагавшегося на лекциях. Решение некоторых (но не обязательно всех) задач повышенной сложности является достаточным условием получения отличной оценки.

IV. ПРИМЕРЫ ОЦЕНОЧНЫХ СРЕДСТВ

Тематика заданий текущего контроля

1. Перечислить в данном кольце вычетов все делители нуля, все обратимые элементы, все нильпотентные и идемпотентные элементы.
2. Найти в данном кольце вычетов обратный к заданному обратимому элементу.
3. Представить данное кольцо вычетов в виде прямого произведения и выписать явные формулы для изоморфизма .
4. Найти обратимый элемент наибольшего порядка в данном кольце вычетов.
5. Проверить неприводимость данного многочлена над данным простым конечным полем.
6. Построить расширение данного простого конечного поля, в котором данный неприводимый над этим полем многочлен будет иметь корень.
7. В условиях предыдущего пункта найти остальные корни.

Вопросы для оценки качества освоения дисциплины

Примерный перечень вопросов к экзамену.

1. Перечислить все неприводимые многочлены данной степени над данным простым конечным полем.
2. Найти период последовательности, задаваемой данным неприводимым многочленом над данным простым конечным полем.
3. Найти минимальный многочлен данного элемента конечного поля и порядок этого элемента в мультипликативной группе поля.

4. Построить неприводимый многочлен над подходящим простым конечным полем, позволяющий генерировать периодическую последовательность с заданным периодом.

V. РЕСУРСЫ

5.1.Основная литература

1. Кострикин А.И. Введение в алгебру. Часть III. Основные структуры М.: Физматлит, 2004.
2. Кострикин А.И. Введение в алгебру. Часть I. Основы алгебры М.: Физматлит, 2000.

5.2. Дополнительная литература

3. Лидл Р., Нидеррайтер Г. Конечные поля. Том 1, М,: Мир 1988
4. Современная прикладная алгебра, Биркгоф Г., Барти Т. Лань, 2005.

5.3 Программное обеспечение

№ п/п	Наименование	Условия доступа
1.	Microsoft Windows 7 Professional RUS Microsoft Windows 10 Microsoft Windows 8.1 Professional RUS	*Из внутренней сети университета (договор)*
2.	Microsoft Office Professional Plus 2010	*Из внутренней сети университета (договор)*
3.	LaTeX пакет верстки научных текстов	*Свободно распространяемый программный продукт*

5.4. Профессиональные базы данных, информационные справочные системы, интернет-ресурсы (электронные образовательные ресурсы)

№ п/п	Наименование	Условия доступа
	Профессиональные базы данных, информационно-справочные системы	
1.	База препринтов Cornell University	*https://arxiv.org/*
2.	База данных зарубежной периодики MathSciNet	*Онлайн доступ из локальной сети НИУ ВШЭ*
	Интернет-ресурсы (электронные образовательные ресурсы)	
1.	Открытое образование	URL: https://openedu.ru/

5.3 Материально-техническое обеспечение дисциплины

Учебные аудитории для лекционных занятий по дисциплине обеспечивают использование и демонстрацию тематических иллюстраций, соответствующих программе дисциплины в составе:

- ПЭВМ с доступом в Интернет (операционная система, офисные программы, антивирусные программы);
- мультимедийный проектор с дистанционным управлением.

Учебные аудитории для самостоятельных занятий по дисциплине оснащены персональными компьютерами, с возможностью подключения к сети Интернет и доступом к электронной информационно-образовательной среде НИУ ВШЭ.