Правительство Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего профессионального образования "Национальный исследовательский университет "Высшая школа экономики"

Факультет Математики

Программа дисциплины

«Математические основы защиты информации»

для направления 01.03.01 «Математика» подготовки бакалавра
для направления 01.04.01 «Математика» подготовки магистра

Автор программы: Артамкин И.В., д.ф.-м.н., artamkin@mail.ru

Рекомендована секцией УМС по математике «___»_____ 2016 г.

Председатель С.М. Хорошкин _____

Утверждена УС факультета математики «___»_____ 2016 г.

Ученый секретарь Ю.М. Бурман _____

Москва, 2016

1 Область применения и нормативные ссылки

Настоящая программа учебной дисциплины устанавливает минимальные требования к знаниям и умениям студента и определяет содержание и виды учебных занятий и отчетности.

Программа предназначена для преподавателей, ведущих данную дисциплину, учебных ассистентов и студентов направления 01.03.01 «Математика» подготовки бакалавра, направления 01.03.01 «Математика» подготовки магистра

Программа разработана в соответствии с:

- ОС НИУ ВШЭ;
- Рабочим учебным планом университета по направлению 01.03.01 «Математика» подготовки бакалавра 01.04.01 «Математика» подготовки магистра, специализации Математика, утвержденным в 2016 г

2 Цели освоения дисциплины

Целями освоения дисциплины «Математические основы защиты информации» являются:

- 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.

3 Компетенции обучающегося, формируемые в результате освоения дисциплины

В результате освоения дисциплины студент должен:

- Получить 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;
- Освоить основные принципы генерации периодических последовательностей;
- Быть готовым использовать изученный материал в последующей профессиональной деятельности.

В результате освоения дисциплины студент осваивает следующие компетенции:

Компетенция	Код по ФГОС/ НИУ	Дескрипторы – основные признаки освоения (показатели достижения результата)	Формы и методы обучения, способствующие формированию и развитию компетенции
умение формулировать результат	ПК-3	Правильно воспроизводит чужие результаты Правильно формулирует собственные результаты	Компетенция формируется в любом сегменте учебного процесса Формируется в процессе активных занятий (участие в семинарах, выполнение курсовых и дипломных работ).

Компетенция	Код по ФГОС/ НИУ	Дескрипторы – основные признаки освоения (показатели достижения результата)	Формы и методы обучения, способствующие формированию и развитию компетенции
умение строго доказать утверждение	ПК-4	Воспроизводит доказательства стандартных результатов, услышанных на лекциях Оценивает строгость и корректность научных текстов	Изучение базового курса За счет повышения обще-физической и математической культуры в процессе обучения
умение грамотно пользоваться языком предметной области	ПК-7	Владеет профессиональной лексикой в области эргодической теории Распознает и воспроизводит названия основных математических структур, возникающих при изучении данной дисциплины, умеет корректно формулировать утверждения и их доказательства	Продумывание и повторение услышанного на семинарах и лекциях. Беседы с преподавателями во время консультаций. Компетенция достигается в процессе накопления опыта работы по данной теме и общения с преподавателями.
понимание корректности постановок задач	ПК-10	Понимает постановки проблем Адекватно оценивает корректность использования тех или иных математических методов, применяемых при формулировке и решении задач	Продумывание базовых понятий курса Вырабатывается в процессе решения задач, самостоятельного чтения, работы над курсовыми заданиями
выделение главных смысловых аспектов в доказательствах	ПК-16	Понимает и воспроизводит ключевые идеи, методы математической теории информации. Обосновывает и оценивает мотивировки и логические ходы доказательств ее основных результатов.	Продумывание ключевых моментов лекций Вырабатывается путем активного решения задач, самообразования, общения с преподавателем

4 Место дисциплины в структуре образовательной программы

Настоящая дисциплина относится к циклу математических и естественно научных дисциплин и блоку дисциплин, обеспечивающих подготовку бакалавра и магистра направления подготовки «Математика»

Для изучения данной дисциплины необходимо хорошее владение школьным курсом математики и основными понятиями базового курса линейной алгебры.

Знания, полученные при изучении данной дисциплины могут быть использованы в дальнейшем при изучении более продвинутых курсов алгебры и прикладных курсов по защите информации, криптографии и теории кодирования, :

5 Тематический план учебной дисциплины

№	Название раздела	Всего часов	Аудиторные часы			Самостоя-тельная работа
			Лекции	Семинары	Практические занятия	
1	Диофантовы уравнения. Алгоритм Евклида.	4	2			2
2	Кольца вычетов. Простейшие свойства.	4	2			2
3	Простейшие алгебраические структуры: группы, кольца, поля.	4	2			2
4	Китайская теорема об остатках. Теоремы Эйлера и Ферма. Функция Эйлера.	4	2			2
5	Кольцо многочленов.	4	2			2
6	Построение фактор-колец кольца многочленов и вычисления в них.	4	2			4
7	Фактор-кольца кольца многочленов и сдвиговый регистр.	6	2			4
8	Конечные поля и генерация периодических последосательностей.	8	4			4
9	Строение конечных полей.	4	2			2
	Итого:	44	20			24

6 Формы контроля знаний студентов

Тип контроля	Форма контроля					Параметры **
		1	2	3	4	
Текущий еженедельно	Решение домашнего задания	1	1	1	1	Письменное задание, выдаваемое студентам на дом. Срок сдачи задания – на следующем занятии.. Срок проверки заданий – неделя.
Итоговый	Экзамен				1	Письменная работа + беседа с преподавателем (всего 1,5-2 часа)

9 письменных домашних заданий
1 экзамен

6.1 Критерии оценки знаний, навыков

Оценки по всем формам текущего контроля выставляются по 10-ти балльной шкале.

Основная форма текущего контроля – решение задач из домашних заданий. 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. Обсуждение подходов к решению этих задач происходит на семинарах и во время консультаций. Решение некоторых (но не обязательно всех) задач повышенной сложности является необходимым условием получения отличной оценки за домашнее задание (8-10 баллов).

Экзамен включает в себя письменную подготовку, состоящую из двух достаточно сложных задач, решение которых требует от студента владения как понятийным, так и техническим аппаратом по изучавшимся в течение модуля темам, а также из одного - двух теоретических вопросов. Студент в очной беседе с преподавателем излагает результаты своей письменной работы и, при необходимости, отвечает на 1-2 дополнительных вопроса. Время, отводимое на беседу: ½ - 1 час во время зачета, и ½ - 1½ часа во время экзамена.

6.2 Порядок формирования оценок по дисциплине

Промежуточная оценка за первый модуль $О_{промежуточная\ 1}$ и накопленная оценка за 2 модуль $О_{накопленная\ 2}$ рассчитываются аналогично:

$$\mathbf{О_{промежуточная\ 1}\ (О_{накопленная\ 2}) = 0.5{*}О_{текущий} + 0.5{*}О_{сам.работа}},$$

где $О_{текущий}$ и $О_{сам.работа}$ --- оценки текущего контроля и самостоятельной работы студентов в соответствующих модулях.

Здесь оценка текущего контроля $О_{текущий}$ рассчитывается как взвешенная сумма трех форм текущего контроля, предусмотренных в РУП

$$\mathbf{О_{текущий} = 0.3{*}О_{д/з} + 0.2{*}О_{к/р} + 0.5{*}О_{кол}},$$

Оценки за домашнее задание $О_{д/з}$, контрольную работу $О_{к/р}$, и коллоквиум $О_{кол}$ выставляются по 10-балльной шкале. Способ округления накопленной оценки текущего контроля: в пользу студента.

Студент, получивший низкие оценки текущего контроля, имеет возможность их однократной пересдачи.

Самостоятельная работа студентов, а именно**:** изучение по поручению преподавателя дополнительных материалов, подготовка на их основе сообщений и выступление с ними на семинарах, а также разбор у доски задач повышенной сложности на семинарских занятиях --- оценивается по 10-бальной шкале оценкой $О_{сам.работа}$. Оценки за самостоятельную работу студента преподаватель выставляет в рабочую ведомость. Накопленная оценка - $О_{сам.\ работа}$ окончательно определяется перед промежуточным (итоговым) контролем.

Накопленная итоговая оценка за весь период изучения дисциплины определяется как среднее арифметическое оценкок за 1 и 2 модули:

$$\mathbf{О_{накопленная\ итоговая} = 0.5{*}(О_{промежут\ 1} + О_{накопленная\ 2})}$$

Результирующая итоговая оценка за дисциплину учитывает также оценку за экзамен $О_{итог.контроль}$, выставляемую по 10-бальной шкале, и определяется по формуле

$$\mathbf{О_{результирующая\ итог} = 0{,}4{*}О_{накопленная\ итоговая} + 0{,}6{*}О_{итог.контроль}}$$

Способ округления накопленной и результирующей итоговых оценок: в пользу студента.

На экзамене(зачете) студент может получить дополнительный вопрос (дополнительную задачу), ответ на который оценивается в 1 балл.

Оценка за итоговый контроль - **блокирующая,** при неудовлетворительной итоговой оценке она равна результирующей.

В диплом ставится результирующая итоговая оценка по учебной дисциплине.

7 Образовательные технологии

На лекции обсуждаются ключевые понятия и технические выкладки разбираемой темы, даются необходимые определения, разбираются поучительные примеры. Студентам на дом даются задачи для самостоятельного разбора, содержащие как упражнения для усвоения пройденного материала, так и нестандартные задачи, позволяющие проверить уровень общего понимания предмета и требующие изучения дополнительного материала. Некоторые задачи предваряют (продолжают) тематику лекций. Студент сдает задачи как в виде письменных домашних работ, так и в виде устной беседы с преподавателем.

8 Оценочные средства для текущего контроля и аттестации студента

8.1 Тематика заданий текущего контроля

Примерный список задач по теме “МОЗИ”.

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.

8.2 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.

9 Учебно-методическое и информационное обеспечение дисциплины

9.1 Базовые учебники

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

9.5 Программные средства

Специальные программные средства не предусмотрены.

9.6 Дистанционная поддержка дисциплины

Специальные дистанционные ресурсы не предусмотрены.

10 Материально-техническое обеспечение дисциплины

Для проведения семинаров не используется специальное оборудование.