МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ ТАДЖИКИСТАН
МЕЖГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКО-ТАДЖИКСКИЙ (СЛАВЯНСКИЙ) УНИВЕРСИТЕТ»

«Утверждаю»
Декан ЕНФ _____
Муродзода Д.С.
«31» 08 2024 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
МАТЕМАТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ И ИНФОРМАЦИОННОЙ БЕЗОПАСТНОСТИ

Направление подготовки: **09.04.03- Прикладная информатика**
Профиль подготовки: **Прикладная информатика в экономике**
Форма подготовки: **очная**
Уровень подготовки: **магистратура**

Душанбе - 2024

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования, утвержденного приказом Министерства образования и науки РФ № 922 от 19.09.2017 г.

При разработке рабочей программы учитываются

- требования работодателей, профессиональных стандартов по направлению / специальности (при наличии) (для общепрофессиональных и профессиональных дисциплин);
- содержание программ дисциплин/модулей, изучаемых на предыдущих и последующих этапах обучения;
- новейшие достижения в данной предметной области.

Рабочая программа обсуждена на заседании кафедры Информатики и ИТ.,
протокол № 1 от 28 августа 2024 г.

Рабочая программа утверждена УМС естественнонаучного факультета,
протокол № 1 от 29 августа 2024 г.

Рабочая программа утверждена Учёным советом естественнонаучного факультета,
протокол № 1 от 30 августа 2024г.

Заведующий кафедрой, к.э.н., доцент _____ Лешукович А.И.

Зам. председателя УМС факультета
к. ф-м.н., доцент _____ Халимов И.И.

Разработчик, к.ф.-м.н., доцент _____ Замонов М.З.

1. ЦЕЛИ И ЗАДАЧИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Данный курс изучается студентами 1-го курса направления 09.0.03 «Прикладная информатика» и направлена на изучение основных сложных алгоритмов и программированию на абстрактные машины. Данный курс входит в систему специализации по направлению информационной безопасности и является продолжением курсов "Основы информационной безопасности" и " Математические основы защиты информации и информационной безопасности".

1.1. Цели изучения дисциплины: является вооружить студентов глубокими знаниями и навыками по разработке методики и составление алгоритмов, и использование программных средств для их решения. Дать научное обоснование понятию «алгоритм» и основы теории сложности алгоритмов, поднять алгоритмическую культуру студентов.

1.2. Задачи изучения дисциплины: являются познакомить студентов с основные знания о математических основах построения криптографических алгоритмов, понятия о вычислительной сложности односторонних функций, используемых в криптографии, методах построения надежных систем защиты и о возможных атаках.

1.3. В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные/ профессиональные / компетенции (элементы компетенций)

Таблица 1.

1) Профессиональные компетенции: проектная деятельность:

Код	**Формируемая компетенция**	**Содержание этапа формирования компетенции**	**Форма контроля**
ПК-5	Способностью разрабатывать и адаптировать прикладное программное обеспечение.	**ИПК-5.1.** Применяет современные технологии разработки и адаптации прикладного программного обеспечения.	Тестирование. Контроль самостоятельной работы. Отчеты по практическим работам. Контрольная работа. Устный опрос.
		ИПК-5.2. Участвует в разработке на современных языках программирования и адаптации прикладного программного обеспечения	
		ИПК-5.3. Применяет современные технологии для разработки веб-приложений	

2.МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП

Дисциплина относится к базовой части профессионального цикла

Курс подготавливает выпускника к работе в современной компании, внедряющей, использующей или разрабатывающей программные средств. Дисциплина логически и содержательно-методически взаимосвязана с дисциплинами ООП, указанных в табл. 2:

Таблица 2.

№	**Название дисциплины**	**Место дисциплины в структуре ООП**
1	*Информатика*	*Б1.О.12*
2	*Математика*	*Б1.О.14*
3	*Дискретная математика*	*Б1.О.15*

4	*Теория вероятности и математическая статистика*	*Б1.О.16*
5	*Операционные системы*	*Б1.О.17*
6	*Практикум по программированию*	*Б1.О.21*

3. СТРУКТУРА И СОДЕРЖАНИЕ КУРСА, КРИТЕРИИ НАЧИСЛЕНИЯ БАЛЛОВ

Объем дисциплины (модуля) составляет 4 зачетных единиц всего 144 часов, из которых: лекции 10 час., практические занятия 32 час., лабораторные работы 0 час., КСР 8 час., всего часов аудиторной нагрузки 42 час., самостоятельная работа 52 час. Контрол-50 час. Экзамен 2 семестр.

3.1 Структура и содержание теоретической части курса:

Тема 1. Алгебраические структуры: группы, кольца, поля.
лекционное занятие (2 часа(ов)):
Введение в алгебраические сруктуры. Определение, свойства, применение алгебраических структур. Группы. Теорема Лагранжа. Конечные поля. Неприволдимые многочлены в конечных полях. Расширения конечных полей.
лабораторная работа (8 часа(ов)):
Решение уравнений в конечных полях. Построение неприводимых многочленов. Нахождение обратных элементов и вычисление частных.
Тема 2. Производящие функции.
лекционное занятие (4 часа(ов)):
Примеры, приводящие к производящим функциям. Реккурентные уравнения. Построение таблицы приводящих функций. Дифферниирование и интегрирование производящих функций.
лабораторная работа (8 часа(ов)):
Использование производящих функций для решения рекккурентных уравнений. Построение реккурентного уравнеия для рядов Фибоначчи. Оценка метода сортировки вставкой.
Тема 3. Мультипликативные функции. Дзета функция Римана.
лекционное занятие (2 часа(ов)):
Молулярная арифметика.Решение сравнений 1 порядка. Эйлера. Формула для вычисления функции Эйлера. Функция Мебиуса. Формула инверсии Мебиуса.
лабораторная работа (8 часа(ов)):
Формула всключений и исключений. Решение задач. Использование формулы для оценки функции распределения простых чисел.
Тема 4. Субэкспоненциальные методы факторизации натуральных чисел.
лекционное занятие (2 часа(ов)):
Эллиптические кривые. Метод Ленстры факторизации натуральных чисел. Выбор параметров метода Ленстры. Факторизация методом решета числового поля.
лабораторная работа (8 часа(ов)):
Выполнение лабораторной работы по факторизации методом Ленстры. Оценка сходмости метода. Выбор параметров первой и второй стадий метода.

Формы контроля и критерии начисления баллов

Контроль усвоения студентом каждой темы осуществляется в рамках балльно-рейтинговой системы (БРС), включающей текущий, рубежный и итоговый контроль. Студенты **1 курсов**, обучающиеся по кредитно-рейтинговой системе обучения, могут полу-

чить максимально возможное количество баллов - 300. Из них на текущий и рубежный контроль выделяется 200 баллов или 49% от общего количества.

На итоговый контроль знаний студентов выделяется 51% или 100 баллов. Из них 16 баллов администрацией могут быть представлены студенту за особые заслуги (призовые места в Олимпиадах, конкурсах, спортивных соревнованиях, выполнение специальных заданий, активное участие в общественной жизни университета).

Порядок выставления баллов: 1-й рейтинг (1-9 неделя по 11,5 баллов = 8 баллов административных, итого 100 баллов), 2-й рейтинг (10-18 неделя по 11,5 баллов = 8 баллов административных, итого 100 баллов), итоговый контроль 100 баллов.

К примеру, за текущий и 1-й рубежный контроль выставляется 100 баллов: лекционные занятия – 20 баллов, за практические занятия (КСР, лабораторные) – 32 балла, за СРС – 20 баллов, требования ВУЗа – 20 баллов, административные баллы – 8 баллов.

В случае пропуска студентом занятий по уважительной причине (при наличии подтверждающего документа) в период академической недели, деканат факультета обращается к проректору по учебной работе с представлением об отработке студентом баллов за пропущенные дни по каждой отдельной дисциплине с последующим внесением их в электронный журнал.

Итоговая форма контроля по дисциплине (зачет, зачет с оценкой, экзамен) проводится как в форме тестирования, так и в традиционной (устной) форме. Тестовая форма итогового контроля по дисциплине предусматривает: для естественнонаучных направлений – 10 тестовых вопросов на одного студента, где правильный ответ оценивается в 10 баллов, для гуманитарных направлений/специальности – 25 тестовых вопросов, где правильный ответ оценивается в 4 балла. Тестирование проводится в электронном виде, устный экзамен на бумажном носителе с выставлением оценки в ведомости по аналогичной системе с тестированием.

4. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

4.1. План-график выполнения самостоятельной работы по дисциплине

Таблица 5.

№ п/п	Объем самостоятельной работы в часах	Тема самостоятельной работы	Форма и вид самостоятельной работы	Форма контроля
1	10 ч.	История развития и поколения ЭВМ; общие понятия об информации; способы представления информации; принципы Фон-Неймана; основные устройства ЭВМ	Реферат. Выполнение индивидуальных заданий	Беседа со студентами
2	10 ч.	Понятие об операционной системе и ее функции. Классы операционных систем (ОС). Системные и прикладные программы. семейства Microsoft Office.	Конспект. Выполнение индивидуальных заданий	Защита выполненных работ
3	10 ч.	Общие сведения об операционной системы Windows. Основные операции в Windows. Режимы работы Windows. Операции с папками. Работа с графическом редактором Paint.	Работа в лаборатории Выполнение индивидуальных заданий	Разработка пакет программ

4	10 ч.	Выполнения совокупности повторяющихся действий. Подпрограмма в программе. Обращение программ к другим подпрограммам	Работа в лаборатории Выполнение индивидуальных заданий	Разработка пакет программ

4.2. Характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению.

Задания для текущего контроля

Реферат, доклад

При подготовке к семинарским занятиям студенты должны подготовить рефераты, в которых они самостоятельно рассматривают тот или иной вопрос истории таджикского народа. Реферат является одним из механизмов отработки первичных навыков научно-исследовательской работы. Тему реферата студент выбирает самостоятельно, из предложенного списка (см. ниже).

Коллоквиум

Коллоквиум - средство контроля усвоения учебного материала темы, раздела или разделов дисциплины, организованное как учебное занятие в виде собеседования преподавателя с обучающимися по изученным ранее темам.

4.3. Требования к реферату, докладу

В работах такого рода должны присутствовать следующие структурные элементы: название темы, план работы, введение, основная содержательная часть, заключение, список использованных источников и литературы.

Во введении непременно следует поставить проблему, обосновать ее актуальность, дать краткую характеристику используемых в работе источников и научных публикаций, четко сформулировать цель и задачи работы. В заключительной части обязательно наличие основных результирующих выводов по затронутым проблемам. Только при соблюдении всех этих требований может оцениваться уже собственно содержательная часть работы. Студент должен не просто предложить реферативный материал, но продемонстрировать умение анализировать исторические источники и историографию.

4.4. Критерии оценки выполнения самостоятельной работы

В основу разработки балльно рейтинговой системы положены принципы, в соответствии с которыми формирование рейтинга магистра осуществляется постоянно в процессе его обучения в университете. Настоящая система оценки успеваемости магистров основана на использовании совокупности контрольных точек, равномерно расположенных на всем временном интервале изучения дисциплины. При этом предполагается разделение всего курса на ряд более или менее самостоятельных, логически завершенных блоков и модулей и проведение по ним промежуточного контроля.

Магистрам выставляются следующие баллы за выполнение задания к ПК:

- оценка «отлично» (10 баллов): контрольные тесты, а также самостоятельно выполненные семестровые задания, выполненные полностью и сданные в срок в соответствии с предъявляемыми требованиями;

- оценка «хорошо» (8-9 баллов): задание выполнено и в целом отвечает предъявляемым требованиям, но имеются отдельные замечания в его оформлении или сроке сдачи;

- оценка «удовлетворительно» (6-7 баллов): задание выполнено не до конца, отсутствуют ответы на отдельные вопросы, имеются отклонения в объеме, содержании, сроке выполнения;

- оценка «неудовлетворительно» (5 и ниже): отсутствует решение задачи, задание переписано (скачано) из других источников, не проявлена самостоятельность при его выполнении.

Текущий контроль осуществляется в ходе учебного процесса по результатам выполнения самостоятельной работы и контрольной работы.

Основными формами текущего контроля знаний являются:

- обсуждение вынесенных в планах практических занятий лекционного материала и контрольных вопросов;
- решение тестов и их обсуждение с точки зрения умения сформулировать выводы, вносить рекомендации и принимать адекватные управленческие решения;
- выполнение контрольной работы и обсуждение результатов;
- участие в дискуссиях в качестве участника и модератора групповой дискуссии по темам дисциплины;
- написание и презентация доклада;
- написание самостоятельной (контрольной) работы.

Для контроля усвоения данной дисциплины учебным планом предусмотрен экзамен. Общее количество баллов по дисциплине - 100 баллов. Распределение баллов на текущий и промежуточный контроль при освоении дисциплины, а также итоговой оценке представлено ниже.

	Недели		**РК 1**	**Недели**		**РК 2**	**Адм. баллы**	**ИК**	**ВСЕГО**
	1-4	5-8		10-13	14-17				
Баллы	9	12	10	12	12	10	5	30	100

5. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО- МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

В данном разделе РПД приводится перечень основной литературы (учебники, учебные пособия, монографии) и перечень дополнительной литературы, в который включаются издания, рекомендуемые для углубленного изучения. В перечень основной литературы должны входить учебники, учебные пособия и монографии, изданные в течение последних 5 лет для гуманитарных, социальных и экономических дисциплин и 10 лет для технических, математических и естественнонаучных дисциплин.

Не менее трех источников основной литературы, указанных в РПД, должны быть доступны обучающимся в одной или нескольких электронно- библиотечных системах (электронных библиотеках), сформированных на основании прямых договорных отношений с правообладателями. В данном случае необходимо привести полное библиографическое описание источника и рабочую гиперссылку на соответствующий электронный ресурс. В список основной литературы также могут быть включены печатные издания, имеющиеся в фондах РТСУ в количестве, предусмотренном соответствующим ФГОС ВО.

5.1. Основная литература

1. Алексеев В.Б. Введение в теорию сложности алгоритмов.М.: Издательство ВМиК МГУ, 2012.
2. Мальцев А.И. Алгоритмы и рекурсивные функции. М.: Наука, 1986.
3. Марков А.А., Нагорный Н.М. Теория алгорифмов. М.: ФАЗИС, 1996.
4. Катленд И. Вычислимость. Введение в теорию рекурсивных функций. М.: Мир, 1983.
5. Макконелл Дж. Анализ алгоритмов. Вводный курс. М.: Техносфера, 2013.
6. Макконелл Дж. Основы современных алгоритмов. М.: Техносфера, 2014.
7. Кормен Т., Лейзерсон Ч., Ривест Р. Алгоритмы: построение и анализ. М.: МЦНМО, 2001.
8. Лавров И.А., Максимова Л.Л. Задачи по теории множеств, математической логике и теории алгоритмов. М.: Физматлит, 2015.
9. Гаврилов Г.П., Сапоженко А.А. Задачи и упражнения по дискретной математике. М.: Физматлит, 2014.
10. Левитин А. Алгоритмы: введение в разработку и анализ. М.: Вильямс, 2014.

5.2. Дополнительная литература

11. Шоломов Л.А. Основы теории дискретных логических и вычислительных устройств. М.: Наука, 1980.
12. Кузнецов О.П. Дискретная математика для инженера. – СПб: Издательство «Лань», 2004.
13. Зубков О.В. Дискретные преобразователи информации. Учебное пособие. – Иркутск. Издательство ИГПУ, 2005.
14. Верещагин И.К., Шень А. Вычислимые функции. М.: МЦНМО, 1999.
15. Рейнгольд Э., Нивергельт Ю., Део Н. Комбинаторные алгоритмы. Теория и практика. М.: Мир, 1980.
16. Сапоженко А.А. Некоторые вопросы сложности алгоритмов. М.: Изд-во ВаиК МГУ, 2001.
17. Ахо А., Хопкрофт Дж., Ульман Дж. Построение и анализ вычислительных алгоритмов. М.: Мир, 1979.

5.3. Нормативно-правовые материалы (по мере необходимости)

5.4. Перечень ресурсов информационно-телекоммуникационной сети Интернет

В данном разделе приводится перечень ресурсов информационно телекоммуникационной сети «Интернет», необходимых для освоения дисциплины, в виде названия сайта, интернет – портала и т.п. и рабочей гиперссылки. Не допускается размещение ресурсов, содержащих материалы, несоответствующие этическим нормам, в том числе в формате баннеров и т.п.

1. Sun Microsystems, Inc. JDK 6 Documentation – Режим доступа: http://java.sun.com/javase/6/docs/www.osborne.com
2. https://habrahabr.ru
3. https://www.java.com/ru
4. www.ibm.com/developerworks/ru
5. https://info.javarush.ru/
6. https://students.uni-vologda.ac.ru
7. https://lifehacker.ru
8. https://javabegin.ru
9. https://biblio-online.ru/
10. http://www.ipr.books.ru.
11. http://www.portal.tpu.ru>f_ic/files/school/materials.
12. http://www.alleng.ru.
13. http://www.cemi.rssi.ru/rus/structur/paoem/main_frm.htm
14. http://www.twirpx.com.
15. http://www.vipbook.pro>pk/pk.
16. http://www.krivaksin>category/программирования

Перечень информационных технологий и программного обеспечения

Используются лицензионное программное обеспечение ОС Windows -7 и программное обеспечение открытого доступа (Open source), среды программирования (Microsoft C++/C#, Java и др.)

6. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Изучение дисциплины должно сопровождаться изложением теоретического материала в соответствии с программой и с использованием современных мультимедийных технологий, а также разбором конкретных теоретических и практических заданий.

При проведении семинаров необходимо организовать современную информационную среду с обеспечением индивидуального доступа студентов к формируемым информационным ресурсам.

При выполнении лабораторных работ используются соответствующие учебно-методические пособия (в них приводятся задания по лабораторным работам, методические указания по их выполнению, справочный материал с примерами программирования). По каждой лабораторной работе оформляется отчет, на основании которого проводится защита работы (цель – оценка уровня освоения учебного материала). Результаты лабораторных работ учитываются при промежуточной и итоговой аттестации по дисциплине.

Для достижения целевых установок дисциплины преподавателю необходимо интегрировать во взаимосвязанный комплекс содержание семинаров и выполнение проектных работ.

Для достижения успеха в освоении дисциплины студент должен самостоятельно выполнять проектные работы, проявлять активность во время аудиторных занятий, демонстрировать способность решать поставленные задачи в оговоренные сроки и стремление оптимизировать предложенные решения, свободно владеть теоретическим материалом, изученным в рамках курса.

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для реализации дисциплины при кафедре информатики и ИС РТСУ имеются 3 компьютерных классов обеспеченные электронными досками.

В Университете созданы специальные условия обучающихся с ограниченными возможностями здоровья - специальные учебники, учебные пособия и дидактические материалы, специальные технические средства обучения коллективного и индивидуального пользования, предоставление услуг ассистента (помощника), оказывающего обучающимся необходимую техническую помощь, проведение групповых и индивидуальных коррекционных занятий, обеспечение доступа в здания организаций и другие условия, без которых невозможно или затруднено освоение дисциплины обучающимися с ограниченными возможностями здоровья.

Обучающимся с ограниченными возможностями здоровья предоставляются бесплатно специальные учебники и учебные пособия, иная учебная литература, а также обеспечивается:

наличие альтернативной версии официального сайта организации в сети "Интернет" для слабовидящих;

присутствие ассистента, оказывающего обучающемуся необходимую помощь;

обеспечение выпуска альтернативных форматов печатных материалов (крупный шрифт или аудиофайлы);

возможность беспрепятственного доступа обучающихся в учебные помещения, столовые, туалетные и другие помещения организации, а также пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проёмов, лифтов).

8. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Форма итоговой аттестации: экзамен.
Форма промежуточной аттестации 1 и 2 рубежный контроль

Варианты контрольной работы

1. Алгебраические структуры: группы, кольца, поля. Теорема Лагранжа о порядке элемента группы.
2. Конечные поля. Расширения конечных полей. Вычисление обратных элементов в поле.
3. Модулярная арифметика. Решение сравнений 1 порядка.
4. Символ Лежандра. Его свойства и вычисление.
5. Производящие функции числовых последовательностей. Определение и основные свойства. Примеры.
6. Дифференцирование и интегрирование производящих функций.
7. Таблица производящих функций.
8. Вычисление производящей функции ряда Фибоначчи.
9. Полные и приведенные системы вычетов в кольце Z_n.
10. Мультипликативные функции. Функция Эйлера. Формула для вычисления функции Эйлера.Теорема Эйлера о порядке элемента в Z_n.
11. Функция Мебиуса. Теорема о сумме значений функции Мебиуса по всем делителям натурального числа n
12. Формула инверсии Мебиуса. Формула включений/исключений. Ее использование для вычисления функции простых чисел $\pi(x)$.
13. Функция Мангольда и ее свойства. Функция деления.
14. Произведение (конволюция) Дирихле. Мультипликативность конволюции мультипликативных функций.
15. Инверсия Дирихле. Теорема об инверсии Дирихле мультипликативной функции.
16. Ряды Дирихле. Дзета-функция Римана. Произведение рядов Дирихле.
17. Теорема Эйлера о сумме ряда обратных квадратов
18. Свойства дзета-функции Римана. Формула произведения Эйлера
19. Формула суммирования Эйлера-Маклорена (без доказательства).
20. Нахождение асимптотической формулы для частичной суммы гармонического ряда и ряда обратных квадратов.
21. Формулы Стирлинга и ее вывод с помощью формулы суммирования Эйлера-Маклорена.
22. Гладкие и гладкостепенные числа. Формула Бухштаба вычисление числа y-гладких чисел.
23. Факторизация натуральных чисел. Метод Ленстры факторизации на эллиптических кривых.
24. Анализ сходимости метода факторизации Ленстры с помощью изучения распределения гладко-степенных чисел.
25. Метод квадратичного решета факторизации натуральных чисел. Основные параметры метода и их выбор.

Вариант контрольной работы.

1. Дано конечное поле GF(p), p=167, и два элемента этого поля a=87, b=134. Найти сумму, разность, произведение и частное.

2. Дано конечное поле GF(p), p=17. Найти наименьший квадратичный невычет 'a' поля GF(p) и и рассмотреть поле GF(p^2),

полученное добавлением к GF(p) корня α уравнения z^2=a. Найти в поле GF(p^2) сумму, разность, произведение и отношение

элементов z1=2+13*α и z2=7+15*α.

3. Дано конечное GF(p), p=11. Найти неприводимый многочлен P(x) степени 3 и определить поле GF(p^3) многочленов степени 2 в этом поле. Найти произведение многочленов (x^2+3*x)(x^2-1) по модулю P(x)

Итоговая система оценок по кредитно-рейтинговой системе с использованием буквенных символов

Оценка по буквенной системе	**Диапазон соответствующих наборных баллов**	**Численное выражение оценочного балла**	**Оценка по традиционной системе**
A	10	95-100	Отлично
A-	9	90-94	
B+	8	85-89	Хорошо
B	7	80-84	
B-	6	75-79	
C+	5	70-74	Удовлетворительно
C	4	65-69	
C-	3	60-64	
D+	2	55-59	
D	1	50-54	
Fx	0	45-49	Неудовлетворительно
F	0	0-44	

Содержание текущего контроля, промежуточной аттестации, итогового контроля раскрываются в фонде оценочных средств, предназначенных для проверки соответствия уровня подготовки по дисциплине требованиям ФГОС ВО.

ФОС по дисциплине является логическим продолжением рабочей программы учебной дисциплины. ФОС по дисциплине прилагается.