МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
"Казанский (Приволжский) федеральный университет"
Институт вычислительной математики и информационных технологий

УТВЕРЖДАЮ
Проректор по образовательной деятельности КФУ
Проф. Д.А. Таюрский
ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ (ДО КФУ)
_____ «___»_____20__г.

подписано электронно-цифровой подписью

Программа дисциплины

Теоретические основы компьютерной безопасности Б1.Б.36

Направление подготовки: 10.03.01 - Информационная безопасность
Профиль подготовки: Безопасность компьютерных систем
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский

Автор(ы):

Ишмухаметов Ш.Т.

Рецензент(ы):

Латыпов Р.Х.

СОГЛАСОВАНО:

Заведующий(ая) кафедрой: Латыпов Р. Х.
Протокол заседания кафедры No ___ от "____" _____ 201__г

Учебно-методическая комиссия Института вычислительной математики и информационных технологий:
Протокол заседания УМК No ____ от "____" _____ 201__г

Регистрационный No 965918

Казань
2018

Содержание

Программу дисциплины разработал(а)(и) профессор, д.н. (доцент) Ишмухаметов Ш.Т. кафедра системного анализа и информационных технологий отделение фундаментальной информатики и информационных технологий , Shamil.Ishmukhametov@kpfu.ru

1. Цели освоения дисциплины

Данный курс входит в систему специализации по направлению информационной безопасности и является продолжением курсов "Основы информационной безопасности". В ходе этого курса студенты должны получить 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.

2. Место дисциплины в структуре основной образовательной программы высшего профессионального образования

Данная учебная дисциплина включена в раздел "Б1.Б.36 Дисциплины (модули)" основной образовательной программы 10.03.01 Информационная безопасность и относится к базовой (общепрофессиональной) части. Осваивается на 3 курсе, 5 семестр.

Данная дисциплина является спецдисциплиной. Читается на 3 курсе. Базируется на знаниях, полученных в курсах алгебры и геометрии, математического анализа, теории вероятностей и основ информационной безопасности. Курс призван дать представление о математическом аппарате обеспечения решения задач безопасности, что является основой для последующих базовых и профессиональных дисциплин по направлению 'Информационная безопасность', например, для курсов 'Теория кодирования', 'Криптографические методы защиты информации' и пр.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОПК-2 (профессиональные компетенции)	способностью применять соответствующий математический аппарат для решения профессиональных задач
ОПК-7 (профессиональные компетенции)	способностью определять виды информации, виды угроз безопасности информации и возможные методы реализации угроз на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты
ПК-11 (профессиональные компетенции)	способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности
ПК-13 (профессиональные компетенции)	способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов
ПК-8 (профессиональные компетенции)	способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-9 (профессиональные компетенции)	способностью участвовать в разработке подсистемы управления информационной безопасностью

В результате освоения дисциплины студент:

1. должен знать:

основные концепции информационной безопасности;

2. должен уметь:

ориентироваться в вопросах разработки надежных систем защит и видах угроз информационной безопасности.

3. должен владеть:

теоретическими знаниями о математических основах построения криптографических алгоритмов;

4. должен демонстрировать способность и готовность:

навыков оценки безопасности информационных систем.

4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет зачетных(ые) единиц(ы) 144 часа(ов).

Форма промежуточного контроля дисциплины: экзамен в 5 семестре.

Суммарно по дисциплине можно получить 100 баллов, из них текущая работа оценивается в 50 баллов, итоговая форма контроля - в 50 баллов. Минимальное количество для допуска к зачету 28 баллов.

86 баллов и более - "отлично" (отл.);

71-85 баллов - "хорошо" (хор.);

55-70 баллов - "удовлетворительно" (удов.);

54 балла и менее - "неудовлетворительно" (неуд.).

4.1 Структура и содержание аудиторной работы по дисциплине/ модулю

Тематический план дисциплины/модуля

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
1.	Тема 1. Введение в теорию чисел. Классы вычетов по простому и составному модулям.	5	2	8	0	2	Письменное домашнее задание
2.	Тема 2. Конечные поля. Расширения полей по простому модулю.	5		6	0	6	Письменное домашнее задание

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
3.	Тема 3. Система шифрования RSA.	5		4	0	6	Контрольная работа Письменное домашнее задание
4.	Тема 4. Сложность криптографических алгоритмов. Задач факторизации целых чисел.	5		4	0	4	Письменное домашнее задание
5.	Тема 5. Дискретное логарифмирование в конечных полях.	5		4	0	6	Письменное домашнее задание
6.	Тема 6. Эллиптические кривые.	5		6	0	6	Письменное домашнее задание
7.	Тема 7. Методы разработки эффективных алгоритмов.	5		4	0	4	Письменное домашнее задание
8.	Тема 8. Решение уравнений 1-й и 2-й степени в конечных полях.	5		0	0	2	Контрольная работа Письменное домашнее задание
.	Тема . Итоговая форма контроля	5		0	0	0	Экзамен
	Итого			36	0	36	

4.2 Содержание дисциплины

Тема 1. Введение в теорию чисел. Классы вычетов по простому и составному модулям.

лекционное занятие (8 часа(ов)):

Системы вычетов. Основная и приведенная системы вычетов. Модульная арифметика. Функция Эйлера и ее вычисление. Функция Мебиуса. Формула обращения. Производящие функции. Решение реккурентных уравнений. Китайская теорема обо остатках.

лабораторная работа (2 часа(ов)):

Производящие функции. Решение реккурентных уравнений.

Тема 2. Конечные поля. Расширения полей по простому модулю.

лекционное занятие (6 часа(ов)):

Конечные поля по простому модулю. Вычисления в конечных полях. Решение уравнений 1-о и 2-о порядка. Символ Лежандра. Символ Якоби. Вычисление квадратных уравнений. Расширения конечных полей. Алгебра полиномов.

лабораторная работа (6 часа(ов)):

Разработка приложения для выполнения вычислений в конечных полях.

Тема 3. Система шифрования RSA.

лекционное занятие (4 часа(ов)):

Введение в RSA. Сложность задачи факторизации. Основные алгоритмы, лежащие в основе RSA. Алгоритм проверки простоты Рабина-Миллера. Псевдопростые числа.

лабораторная работа (6 часа(ов)):

Разработка приложения для шифрования сообщений по методу RSA.

Тема 4. Сложность криптографических алгоритмов. Задач факторизации целых чисел.

лекционное занятие (4 часа(ов)):

Введение в теорию сложности алгоритмов. Алгоритмы факторизации Ферма, ро-метод Полларда, (p-1)-метод Полларда. Экспоненциальные и субэкспоненциальные алгоритмы.

лабораторная работа (4 часа(ов)):

Разработка приложения для факторизации длинных чисел по методам Полларда и Ферма. .

Тема 5. Дискретное логарифмирование в конечных полях.

лекционное занятие (4 часа(ов)):

Сложность задачи дискретного логарифмирования в конечном поле. Методы вычисления дискретного логарифма: метод "гигантских" и "детских" шагов Шенкса, методы, основанные на китайской теореме обо остатках, метод Полларда.

лабораторная работа (6 часа(ов)):

Разработка приложения для вычисления дискретного логарифма.

Тема 6. Эллиптические кривые.

лекционное занятие (6 часа(ов)):

Введение в эллиптические кривые. Операции сумммирования и уудвоения точек на ЭК. Проективные координаты для ЭК. Эффективнеы алгоритмы для вычислений точек ЭК. Порядок кривой. Неравенство Хассе.

лабораторная работа (6 часа(ов)):

Разработка приложения для шифрования с использование эллиптических кривых.

Тема 7. Методы разработки эффективных алгоритмов.

лекционное занятие (4 часа(ов)):

Алгоритм Евклида для вычисления наибольшего общего делителя и его модификации. Бинарный и k-арныйалгоритмы. Представление схемы вычисления НОД в в виде непрерывной дроби. Оценки среднего числа итераций в алгоритме Евклида.

лабораторная работа (4 часа(ов)):

Разработка приложения для оценки эффективности алгоритма Евклида.

Тема 8. Решение уравнений 1-й и 2-й степени в конечных полях.

лабораторная работа (2 часа(ов)):

Вычисление обратных элементов. Нахождение квадратичных вычетов и примитивных элементов поля. Вычисление символа Лежандра. Закон квадратичной взаимности Гаусса.

4.3 Структура и содержание самостоятельной работы дисциплины (модуля)

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
1.	Тема 1. Введение в теорию чисел. Классы вычетов по простому и составному модулям.	5	2	подготовка домашнего задания	6	домашнее задание

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
2.	Тема 2. Конечные поля. Расширения полей по простому модулю.	5		подготовка домашнего задания	6	домашнее задание
3.	Тема 3. Система шифрования RSA.	5		подготовка домашнего задания	3	домашнее задание
				подготовка к контрольной работе	3	контрольная работа
4.	Тема 4. Сложность криптографических алгоритмов. Задач факторизации целых чисел.	5		подготовка домашнего задания	4	домашнее задание
5.	Тема 5. Дискретное логарифмирование в конечных полях.	5		подготовка домашнего задания	4	домашнее задание
6.	Тема 6. Эллиптические кривые.	5		подготовка домашнего задания	4	домашнее задание
7.	Тема 7. Методы разработки эффективных алгоритмов.	5		подготовка домашнего задания	2	домашнее задание
8.	Тема 8. Решение уравнений 1-й и 2-й степени в конечных полях.	5		подготовка домашнего задания	2	домашнее задание
				подготовка к контрольной работе	2	контрольная работа
	Итого				36	

5. Образовательные технологии, включая интерактивные формы обучения

Обучение происходит в форме лекционных и лабораторных занятий, а также самостоятельной работы студентов.

Теоретический материал излагается на лекциях. Причем конспект лекций, который остается у студента в результате прослушивания лекции не может заменить учебник. Его цель-формулировка основных утверждений и определений. Прослушав лекцию, полезно ознакомиться с более подробным изложением материала в учебнике. Список литературы разделен на две категории: необходимый для сдачи экзамена минимум и дополнительная литература.

Изучение курса подразумевает не только овладение теоретическим материалом, но и получение практических навыков для более глубокого понимания разделов на основе решения задач и упражнений, иллюстрирующих доказываемые теоретические положения, а также развитие абстрактного мышления и способности самостоятельно доказывать утверждения.

Самостоятельная работа предполагает выполнение домашних работ. Практические задания, выполненные в аудитории, предназначены для указания общих методов решения задач определенного типа. Закрепить навыки можно лишь в результате самостоятельной работы.

Кроме того, самостоятельная работа включает подготовку к экзамену. При подготовке к сдаче экзамена весь объем работы рекомендуется распределять равномерно по дням, отведенным для подготовки к экзамену, контролировать каждый день выполнения работы. Лучше, если можно перевыполнить план. Тогда будет резерв времени.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

Тема 1. Введение в теорию чисел. Классы вычетов по простому и составному модулям.

домашнее задание , примерные вопросы:

Углубленное изучение литературы по изучаемой теме. Выполнить действия с элементами Zn. Решение задачи на вычисление обратных элементов по модулю

Тема 2. Конечные поля. Расширения полей по простому модулю.

домашнее задание , примерные вопросы:

Решение типовых задач. Вычисление симолов Лежандра и Якоби. Нахождение квадратичных вычетов, построение конечных рамширнений.

Тема 3. Система шифрования RSA.

домашнее задание , примерные вопросы:

Углубленное изучение литературы по изучаемой теме. Разобрать тест Миллера-Рабина. Выполнить построение системы ключей RSA и пробное шифрование/расшифрование.

контрольная работа , примерные вопросы:

Вариант контрольной работы 1. 1. Выполнить тест Миллера-Рабина для n=41. 2. Даны два простых числа p и q. Найти остальные параметры RSA, выполнить шифрование строки данных. 3. Используя метод Ферма, выполнить взлом ключа RSA и расшифровать секретный пароль.

Тема 4. Сложность криптографических алгоритмов. Задач факторизации целых чисел.

домашнее задание , примерные вопросы:

Изучить методы факторизации Ферма, Полларда, решить тестовые задачи по теме.

Тема 5. Дискретное логарифмирование в конечных полях.

домашнее задание , примерные вопросы:

Изучить методы вычисления дискретногог логарифма. Решение задач на вычисление дискретного логарифма по методу гигантских и малых шагов Шенкса.

Тема 6. Эллиптические кривые.

домашнее задание , примерные вопросы:

Углубленное изучение литературы по изучаемой теме. Выполнить псотроение эллиптических кривых, оценить число точек на кривой, выполнить операции сложения и удвоения на точках эллиптической кривой.

Тема 7. Методы разработки эффективных алгоритмов.

домашнее задание , примерные вопросы:

Рассмотреть алгоритмы сведения решения задач к подзадачам. Решение реккурентных уранений с использованием производящих функций.

Тема 8. Решение уравнений 1-й и 2-й степени в конечных полях.

домашнее задание , примерные вопросы:

Подготока к контрольной работе. Решение задач на вычисления в конечных полях.

контрольная работа , примерные вопросы:

Вариант контрольной работы 2. 1. Решить уравнение 2-й степени в конечном поле. 2. Вычислить символ Лежандра для заданного элемента в кольце вычетов. 3. Решить реккурентное уравнение с использованием производящих функций.

Итоговая форма контроля

экзамен (в 5 семестре)

Примерные вопросы к экзамену:

1. Классы вычетов Zn по модулю n. Полная и приведенная система вычетов. Теоремы об умножении элементов полной и приведенной системы на число.
2. Функция Эйлера. Теорема Эйлера. Вычисление функции Эйлера.
3. Мультипликативные функции. Функция Мебиуса. Ее свойства. Формула обращения Мебиуса.
4. Решение сравнений первого порядка по простому и составному модулям.
5. Символ Лежандра. Его свойства. Алгоритм вычисления символа Лежандра.
6. Квадратичные вычеты. Вычисление квадратных корней в Zn. Алгоритм Шенкса вычисления квадратного корня.
7. Конечные поля. Вычисления в конечных полях. Теорема о существовании примитивного элемента.
8. Дискретное логарифмирование в конечных полях. Алгоритм Шенкса "гигантских" и "детских" шагов.
9. Другие методы дискретного логарифмирования. Метод Полларда и его оценка его эффективности.
10. Расширения конечных полей. Неприводимые многочлены. Структура расширения конечного поля. Вычисление обратного элемента.
11. Тест Миллера-Рабина проверки простоты натурального числа. Оценки его точности.
12. Метод RSA. Шифрование и электронные подписи на основе RSA. Алгоритм быстрого возведения в степень.
13. Алгоритмы факторизации. (p-1)-метод Полларда и оценка его эффективности.
14. Другие методы факторизации. Ро-метод Полларда и оценка его эффективности.
15. Эллиптические кривые. Операции сложения точек эллиптической кривой.
16. Криптографические протоколы на ЭК.
17. Эллиптические кривые в проективных координатах. Формулы для суммы точек и удвоения в проективных координатах.
18. Алгоритм Евклида вычисления Н.О.Д двух целых чисел и его расширенная версия. Оценка его сложности.
19. Бинарная версия алгоритма Евклида и его сложность.
20. k-арный алгоритм Евклида и его сложность Сравнение k-арного и классического алгоритмов.

7.1. Основная литература:

1. Ишмухаметов Ш.Т. Математические основы защиты информации: учебное пособие, 2012. - URL: http://kpfu.ru/docs/F366166681/mzi.pdf
2. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2014. - 432 с. URL: http://www.znanium.com/bookread.php?book=420047
3. Информационная безопасность и защита информации: Учебное пособие/Баранова Е. К., Бабаш А. В., 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с. URL:http://znanium.com/bookread2.php?book=495249
4. Нестеров, С.А. Основы информационной безопасности [Электронный ресурс] : учебное пособие. - Электрон. дан. - СПб. : Лань, 2016. - 324 с. - Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=75515
5. Информационная безопасность конструкций ЭВМ и систем: учебное пособие / Е.В. Глинская, Н.В. Чичварин. - М.: НИЦ ИНФРА-М, 2016. - 118 с. http://znanium.com/bookread2.php?book=507334

7.2. Дополнительная литература:

1. Гришина Н. В. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - 2-е изд., доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 240 с. - ЭБС 'Знаниум': http://znanium.com/bookread.php?book=491597

2. Хорев П. Б. Программно-аппаратная защита информации: учебное пособие / П.Б. Хорев. - М.: Форум, 2009. - 352 с. - ЭБС 'Знаниум': http://znanium.com/bookread.php?book=169345

3. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: ИНФРА-М, 2012. - 416 с. URL: http://znanium.com/bookread.php?book=335362

4. Основные положения информационной безопасности: Учебное пособие/В.Я.Ищейнов, М.В.Мецатунян - М.: Форум, НИЦ ИНФРА-М, 2015. - 208 с. ЭБС 'Знаниум': http://znanium.com/bookread2.php?book=508381

7.3. Интернет-ресурсы:

Интернет-портал образовательных ресурсов по ИТ - http://www.intuit.ru

Интернет-портал ресурсов по математике - http://www.math.ru

Электронная библиотека ресурсов по техническим наукам - http://techlibrary.ru

электронное пособие - http://www.ksu.ru/f9/bin_files/metod_tzis!113.doc

электронное пособие - http://www.ksu.ru/f9/bibl/Monograph_ishm.pdf

8. Материально-техническое обеспечение дисциплины(модуля)

Освоение дисциплины "Теоретические основы компьютерной безопасности" предполагает использование следующего материально-технического обеспечения:

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен студентам. ЭБС "ZNANIUM.COM" содержит произведения крупнейших российских учёных, руководителей государственных органов, преподавателей ведущих вузов страны, высококвалифицированных специалистов в различных сферах бизнеса. Фонд библиотеки сформирован с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, УМК, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. В настоящее время ЭБС ZNANIUM.COM соответствует всем требованиям федеральных государственных образовательных стандартов высшего профессионального образования (ФГОС ВПО) нового поколения.

лекции и лабораторные занятия по дисциплине проводятся в аудитории, оснащенной доской и мелом (маркером)

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 10.03.01 "Информационная безопасность" и профилю подготовки Безопасность компьютерных систем .

Автор(ы):
Ишмухаметов Ш.Т. _____
"__" _____ 201 __ г.

Рецензент(ы):
Латыпов Р.Х. _____
"__" _____ 201 __ г.