МИНПРОСВЕЩЕНИЯ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования "Тульский государственный педагогический университет им. Л.Н. Толстого"

(ФГБОУ ВО "ТГПУ им. Л.Н. Толстого")

Основы криптоанализа

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **кафедра алгебры, математического анализа и геометрии**

ОПОП **Направление 02.03.01 Математика и компьютерные науки**
направленность (профиль) Математические основы компьютерных наук

Квалификация **Бакалавр**

Год начала подготовки **2022**

Форма обучения **очная**

Общая трудоемкость **3 з.е.**

Виды контроля по семестрам:
зачет 6

Семестр(Курс.Номер семестра на курсе)	**6(3.2)**		Итого	
	УП	РПД	УП	РПД
Лекции	18	18	18	18
Лабораторные	24	24	24	24
Итого ауд.	42	42	42	42
КСР	2	2	2	2
Контактная работа	44	44	44	44
Сам. работа	64	64	64	64
Часы на контроль	0	0	0	0
Практическая подготовка	0	0	0	0
Семинары	0	0	0	0
Консультации	0	0	0	0
Итого трудоемкость в часах	108	108	108	108

Программу составил(и):

Рабочая программа дисциплины

Основы криптоанализа

разработана в соответствии с ФГОС:

Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 02.03.01 Математика и компьютерные науки (приказ Минобрнауки России от 23.08.2017 г. № 807)

составлена на основании учебного плана:

Направление 02.03.01 Математика и компьютерные науки
направленность (профиль) Математические основы компьютерных наук
утвержденного Учёным советом вуза от 28.02.2022 протокол № 3.

РПД утверждена Учёным советом университета
протокол от 1.1.1 г. №

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ
Знакомство с основами криптоанализа

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	Б1.В.ДЭ.04
2.1	**Требования к предварительной подготовке обучающегося:**
1.	Веб-программирование
2.	Интеллектуальный анализ данных и методы поддержки принятия решений
3.	Практикум по программированию мобильных приложений
4.	Теория чисел и элементы криптографии
5.	Базы данных и СУБД
6.	Методы и технологии программирования
7.	Операционные системы
8.	Программирование
9.	Архитектура вычислительных систем
10.	вычислительная практика
11.	Вычислительные сети
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
1.	Моделирование бизнес-процессов
2.	научно-исследовательская работа
3.	Научные основы курса элементарной алгебры
4.	Параллельное программирование
5.	Компьютерное моделирование
6.	преддипломная практика

3. СООТНЕСЕНИЕ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ) С ИНДИКАТОРАМИ ДОСТИЖЕНИЯ КОМПЕТЕНЦИЙ	
3.1 Компетенции обучающегося и индикаторы их достижения:	
ОПК-4: Способен находить, анализировать, реализовывать программно и использовать на практике математические алгоритмы, в том числе с применением современных вычислительных систем	
ОПК-4.1	Знает основные понятия, гипотезы, теоремы, методы, математические и алгоритмические модели, составляющие содержание фундаментальной и прикладной математики и связанные с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности
	Знает основные методы решения задач криптоанализа.
ОПК-4.2	Умеет осуществлять поиск, анализ и программную реализацию математических алгоритмов
	Умеет осуществлять программную реализацию алгоритмов криптоанализа.
ОПК-4.3	Владеет навыками программной реализации математических алгоритмов с применением современных вычислительных систем
	Владеет навыками программной реализации алгоритмов криптоанализа
ПК-2: Способен разрабатывать требования и проектировать программное обеспечение	
ПК-2.1	Знает методологии разработки программного обеспечения и технологии программирования
	Знает методы анализа алгоритмов криптоанализа.
ПК-2.2	Умеет проводить оценку и обоснование рекомендуемых решений
	Умеет проводить анализ алгоритмов необходимых для решения конкретных задач криптоанализа.
ПК-2.3	Владеет навыками разработки технических спецификаций на программные компоненты и их взаимодействие
	Имеет опыт разработки технических спецификаци на реализации алгоритмов криптоанализа.
3.2 Результаты обучения по дисциплине: **В результате освоения дисциплины обучающийся должен:**	
	Знать:
З.1	Знает основные методы решения задач криптоанализа.
З.2	Знает методы анализа алгоритмов криптоанализа.
	Уметь:

У.1	Умеет осуществлять программную реализацию алгоритмов криптоанализа.
У.2	Умеет проводить анализ алгоритмов необходимых для решения конкретных задач криптоанализа.
	Владеть:
В.1	Владеет навыками программной реализации алгоритмов криптоанализа
В.2	Имеет опыт разработки технических спецификаци на реализации алгоритмов криптоанализа.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Литература	Содержание
	Математические основы криптографии				
1.1	Математические основы криптографии /Лек/	6	2		Математические основы криптографии. Теория делимости. Модульная арифметика и дискретный логарифм.
1.2	Математические основы криптографии /Лаб/	6	2		Математические основы криптографии. Теория делимости. Модульная арифметика и дискретный логарифм.
	Теория кодирования				
2.1	Линейные блоковые коды. Код Хэмминга /Лек/	6	2		Двоичный код. Расстояние Хэмминга. Кодовое расстояние. Линейный код. Порождающая матрица. Проверочная матрица. Код Хэмминга и его свойства.
2.2	Линейные блоковые коды. Код Хэмминга /Лаб/	6	2		Двоичный код. Расстояние Хэмминга. Кодовое расстояние. Линейный код. Порождающая матрица. Проверочная матрица. Код Хэмминга и его свойства.
2.3	Циклические коды. Аппаратная реализация кодирования и декодирования. Коды БЧХ /Лек/	6	2		Определение циклического кода, свойства. Архитектура кодера и декодера для цилического кода. Код Боуза-Чоудхури-Хоквингема.
2.4	Циклические коды. Аппаратная реализация кодирования и декодирования. Коды БЧХ /Лаб/	6	2		Определение циклического кода, свойства. Архитектура кодера и декодера для цилического кода. Код Боуза-Чоудхури-Хоквингема.
2.5	Мажоритарное декодирование и коды Рида-Маллера. Недвоичные коды и коды Рида-Соломона /Лек/	6	2		Мажоритарное декодирование линейных кодов. Коды Рида-Маллера, их свойства. Недвоичные циклические коды. Код Рида-Соломона, его свойства.
2.6	Мажоритарное декодирование и коды Рида-Маллера. Недвоичные коды и коды Рида-Соломона /Лаб/	6	4		Мажоритарное декодирование линейных кодов. Коды Рида-Маллера, их свойства. Недвоичные циклические коды. Код Рида-Соломона, его свойства.
	Основы симметричного шифрования				
3.1	Шифры перестановки. Шифры замены. Поточные и блочные шифры. /Лек/	6	2		Разновидности шифров перестановки. Одноалфавитные и многоалфавитные замены. Вопросы криптоанализа простейших шифров.
3.2	Шифры перестановки. Шифры замены. Поточные и блочные шифры. /Лаб/	6	4		Разновидности шифров перестановки. Одноалфавитные и многоалфавитные замены. Вопросы криптоанализа простейших шифров.
3.3	Шенноновские модели криптосистем /Лек/	6	2		Теоретико-информационный подход к оценке криптостойкости шифров. Криптографическая стойкость шифров. Надежность ключей и сообщений. Совершенные шифры.

3.4	Шенноновские модели криптосистем /Лаб/	6	2		Теоретико-информационный подход к оценке криптостойкости шифров. Криптографическая стойкость шифров. Надежность ключей и сообщений. Совершенные шифры.
	Шифрование с открытым ключом				
4.1	Криптосистемы RSA и Эль-Гамаля /Лек/	6	2		Понятие односторонней функции и односторонней функции с «лазейкой». Криптосистемы RSA и Эль-Гамаля. Проблемы факторизации целых чисел и логарифмирования в конечных полях. Секретные характеристики в системах с открытым ключом.
4.2	Криптосистемы RSA и Эль-Гамаля /Лаб/	6	4		Понятие односторонней функции и односторонней функции с «лазейкой». Криптосистемы RSA и Эль-Гамаля. Проблемы факторизации целых чисел и логарифмирования в конечных полях. Секретные характеристики в системах с открытым ключом.
4.3	Электронная цифровая подпись /Лаб/	6	2		Понятие ЭЦП. Стандарты ЭЦП. Однонаправленные функции и методы их построения.
4.4	Электронная цифровая подпись /Лек/	6	2		Понятие ЭЦП. Стандарты ЭЦП. Однонаправленные функции и методы их построения.
4.5	Проблема распределения ключей и протоколы распределения ключей /Лек/	6	2		Проблема распределения ключей и протоколы распределения ключей
4.6	Проблема распределения ключей и протоколы распределения ключей /Лаб/	6	2		Проблема распределения ключей и протоколы распределения ключей
	КСРС				
5.1	КСРС /КСР/	6	2		КСРС
	Самостоятельная работа				
6.1	Самостоятельная работа /Ср/	6	64		Самостоятельная работа

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

5.1. Типовые задания для проведения текущего контроля

Вопросы к зачету

1. Криптография и криптоанализ: основные понятия и этапы развития
2. Элементарные шифры.
3. Потоковые шифры.
4. Блочные шифры.
5. Симметричные криптосистемы.
6. Стандарт шифрования AES.
7. Особенности применения алгоритмов симметричного шифрования.
8. Асимметричные криптосистемы.
9. Алгоритм шифрования RSA.
10. Функции хеширования: назначение и использование.
11. Отечественный стандарт хеширования ГОСТ Р 3411-94.
12. Основные процедуры цифровой подписи.
13. Электронная подпись RSA.
14. Электронная подпись на базе шифра Эль-Гамаля.
15. Метод распределения ключей Диффи-Хеллмана.
16. Основные положения теории информации.
17. Математические основы кодирования и декодирования.
18. Коды с исправлением и обнаружением ошибок.
19. Линейные коды.
20. Циклические коды.

5.2. Типовые задания для проведения промежуточной аттестации

Вопросы к зачету

1. Криптография и криптоанализ: основные понятия и этапы развития
2. Элементарные шифры.
3. Потоковые шифры.
4. Блочные шифры.
5. Симметричные криптосистемы.
6. Стандарт шифрования AES.
7. Особенности применения алгоритмов симметричного шифрования.
8. Асимметричные криптосистемы.
9. Алгоритм шифрования RSA.
10. Функции хеширования: назначение и использование.
11. Отечественный стандарт хеширования ГОСТ Р 3411-94.
12. Основные процедуры цифровой подписи.
13. Электронная подпись RSA.
14. Электронная подпись на базе шифра Эль-Гамаля.
15. Метод распределения ключей Диффи-Хеллмана.
16. Основные положения теории информации.
17. Математические основы кодирования и декодирования.
18. Коды с исправлением и обнаружением ошибок.
19. Линейные коды.
20. Циклические коды.

5.3. Перечень видов оценочных средств

Задания для лабораторных занятий
Контрольная работа
Зачет

5.4. Процедура применения оценочных материалов

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.3.Информационные технологии

6.3.1 Перечень лицензионного и свободно распространяемого программного обеспечения

6.3.2 Перечень информационных справочных систем и профессиональных баз данных

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)