МИНПРОСВЕЩЕНИЯ РОССИИ

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

(ФГБОУ ВО "ТГПУ им. Л.Н. Толстого")

Криптография и кодирование

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

Криптография и кодирование

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
Познакомить студентов с основными понятиями и методами криптографии и кодирования.

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

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
	основные положения теории криптографии и кодирования. основы теории информации классификацию основных систем шифрования
ОПК-4.2	Умеет осуществлять поиск, анализ и программную реализацию математических алгоритмов
	применять полученные знания к исследованию простейших систем шифрования квалифицированно оценивать область применения конкретных механизмов криптографической защиты для построения защищенных информационных систем
ОПК-4.3	Владеет навыками программной реализации математических алгоритмов с применением современных вычислительных систем
	навыками построения моделей простейших систем шифрования навыками проектирования подсистем и средств обеспечения криптографической безопасности информации и участвовать в проведении технико-экономического обоснования соответствующих проектных решений
ПК-2: Способен разрабатывать требования и проектировать программное обеспечение	
ПК-2.1	Знает методологии разработки программного обеспечения и технологии программирования
	основные положения теории криптографии и кодирования. основы теории информации классификацию основных систем шифрования
ПК-2.2	Умеет проводить оценку и обоснование рекомендуемых решений
	применять полученные знания к исследованию простейших систем шифрования квалифицированно оценивать область применения конкретных механизмов криптографической защиты для построения защищенных информационных систем
ПК-2.3	Владеет навыками разработки технических спецификаций на программные компоненты и их взаимодействие

	навыками построения моделей простейших систем шифрования навыками проектирования подсистем и средств обеспечения криптографической безопасности информации и участвовать в проведении техникоэкономического обоснования соответствующих проектных решений

3.2 Результаты обучения по дисциплине:
В результате освоения дисциплины обучающийся должен:

	Знать:
З.1	основные положения теории криптографии и кодирования.
З.2	основы теории информации
З.3	классификацию основных систем шифрования
	Уметь:
У.1	применять полученные знания к исследованию простейших систем шифрования
У.2	квалифицированно оценивать область применения конкретных механизмов криптографической защиты для построения защищенных информационных систем
	Владеть:
В.1	навыками построения моделей простейших систем шифрования
В.2	навыками проектирования подсистем и средств обеспечения криптографической безопасности информации и участвовать в проведении техникоэкономического обоснования соответствующих проектных решений

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		
1.2	Математические основы криптографии /Лаб/	6	4		
	Теория кодирования				
2.1	Линейные блоковые коды. Код Хэмминга /Лек/	6	2		
2.2	Линейные блоковые коды. Код Хэмминга /Лаб/	6	2		
2.3	Циклические коды. Аппаратная реализация кодирования и декодирования. Коды БЧХ. /Лек/	6	2		
2.4	Циклические коды. Аппаратная реализация кодирования и декодирования. Коды БЧХ. /Лаб/	6	2		
2.5	Мажоритарное декодирование и коды Рида-Маллера. Недвоичные коды и коды Рида-Соломона /Лек/	6	2		
2.6	Мажоритарное декодирование и коды Рида-Маллера. Недвоичные коды и коды Рида-Соломона /Лаб/	6	2		
	Основы симметричного шифрования				
3.1	Шифры перестановки. Шифры замены. Поточные и блочные шифры /Лек/	6	2		

3.2	Шифры перестановки. Шифры замены. Поточные и блочные шифры /Лаб/	6	4		
3.3	Шенноновские модели криптосистем /Лек/	6	2		
3.4	Шенноновские модели криптосистем /Лаб/	6	2		
	Шифрование с открытым ключом				
4.1	Криптосистемы RSA и Эль-Гамаля /Лек/	6	2		
4.2	Криптосистемы RSA и Эль-Гамаля /Лаб/	6	4		
4.3	Электронная цифровая подпись /Лек/	6	2		
4.4	Электронная цифровая подпись /Лаб/	6	2		
4.5	Проблема распределения ключей и протоколы распределения ключей /Лек/	6	2		
4.6	Проблема распределения ключей и протоколы распределения ключей /Лаб/	6	2		
	КСРС				
5.1	КСРС /КСР/	6	2		
	Самостоятельная работа				
6.1	Самостоятельная работа /Ср/	6	64		

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

5.1. Типовые задания для проведения текущего контроля

5.2. Типовые задания для проведения промежуточной аттестации

5.3. Перечень видов оценочных средств

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.

5.4. Процедура применения оценочных материалов

Составляющие итоговой оценки за дисциплину:
1) Текущий контроль (общий вес 70 баллов):

до 20 балла – посещение занятий;
до 40баллов – выполнение заданий в ходе выполнения лабораторных работ в LMS Moodle и заданий для самостоятельной работы
до 10 баллов – выполнение отдельно выделенных в методических указаниях к выполнению работ задач повышенной сложности
до 10 баллов – выполнение контрольной работы
Итоговый контроль заключается в проведении зачета (общий вес - 30 баллов). Зачет проводится по вопросам с обязательным решением задач. Как правило, студент получает два вопроса из приведенного выше списка и одну задачу, готовится в присутствии преподавателя и дает подробные комментарии. Студент, пропускавший занятия в ходе семестра, получает дополнительные вопросы и задачи по каждой пропущенной им теме (на усмотрение преподавателя).
Для получения положительной итоговой оценки на зачете необходимо получить не менее 50% по каждой составляющей и выполнить все лабораторные работы. Шкала перевода баллов в оценку: до 40 - «не зачтено»; 41 - 100 - «зачтено».
Промежуточная аттестация может проводиться с применением электронного обучения и (или) дистанционных образовательных технологий в соответствии с «Порядком проведения промежуточной аттестации с применением электронного обучения и /или дистанционных образовательных технологий».

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

1.	Операционная система Microsoft Windows XP Professional Russian. Лицензия № 16698685 от 08.08.2003 г.
2.	Операционная система Microsoft Windows Professional 7 Russian. Лицензия №48497058 от 13.05.2011 г., договор № Пр/16/6 от 05 апреля 2016 г.
3.	Операционная система Microsoft Windows 10 Professional Russian. Контракт № ПР/ФЕН/15/18 от 23.10.2015 г., договор № Пр/16/6 от 05 апреля 2016 г.
4.	Программное обеспечение Microsoft Office Enterprise 2007 Russian. Лицензия №46138962 от 16.11.2009
5.	Программное обеспечение Microsoft Office 2013 Professional. Контракт № 405535 от 2 ноября 2015 года, контракт № ПР/ФЕН/15/18 от 23.10.2015 г.
6.	Программа для распознавания текста ABBYY FineReader 9.0 Corporate Edition. Лицензионный сертификат - код позиции AF90-3U1V25-102, ABBYY FineReader 9.0 Corporate Edition Volume License Concurrent от 28 июля 2009 г.
7.	Электронный словарь ABBYY Lingvo X3 Европейская версия - Код позиции AL14-2U1V05-102, ABBYY Lingvo x3 Европейская версия. Именная лицензия Concurrent от 28 июля 2009 г.
8.	Комплексная система антивирусной защиты Kaspersky Endpoint Security для бизнеса – стандартный Russian Edition. 500-999 Node 2 year Educational Renewal License. Лицензия № 13C8-190514-084943-783-1256 от 15.05.2019
9.	Браузеры Google Chrome, Mozilla, Opera. Свободно распространяемое ПО
10.	Программа просмотра файлов формата RPD Adobe Acrobat Reader DC. Свободно распространяемое ПО
11.	Система облачного хранилища Dropbox. Свободно распространяемое ПО

6.3.2 Перечень информационных справочных систем и профессиональных баз данных

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Ауд.	Назначение	Оборудование и технические средства обучения	Вид
4-301	Лекционная	доска учебная, стол преподавателя, столы учебные	

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

Дисциплина «Криптография и кодирование» направлена на формирование систематизированных теоретических и практических знаний в области криптографии и криптоанализа. Самостоятельная работа студентов по дисциплине составляет 50% от всего объема часов, отводимого учебным планом на изучение дисциплины. В связи с этим успешное изучение материала данного курса в значительной степени зависит от качества самостоятельной подготовки студентов. С целью активизации самостоятельной работы студентов на каждом практическом занятии повторяется соответствующий теоретический материал и закрепляются основные навыки и умения владением математическим аппаратом.
В начале изучения курса студенты получают темы и вопросы лабораторных занятий.