МИНОБРНАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ
Директор института прикладной
математики и компьютерных наук
А.В. Замятин
«02» июня 2021 г.

Теоретико-числовые методы в криптографии

рабочая программа дисциплины

Закреплена за кафедрой	*компьютерной безопасности*
Учебный план	*10.05.01 Компьютерная безопасность,* *профиль «Анализ безопасности компьютерных систем»*
Форма обучения	*очная*
Общая трудоёмкость	*9 з.е.*
Часов по учебному плану	*324*
в том числе:	
аудиторная контактная работа	*143*
самостоятельная работа	*181*
Вид(ы) контроля в семестрах *экзамен/зачет/зачет с оценкой*	*Семестр 6 – экзамен* *Семестр 7 –экзамен*

Томск-2021

Программу составил:
канд. техн. наук, доцент,
зав. кафедры компьютерной безопасности С.А. Останин

Рецензент:
канд. физ.-мат. наук, доцент,
доцент кафедры компьютерной безопасности Е.Г. Пахомова

Рабочая программа дисциплины «Теоретико-числовые методы в криптографии» разработана в соответствии с образовательным стандартом высшего образования – специалитет, самостоятельно устанавливаемым федеральным государственным автономным образовательным учреждением высшего образования «Национальный исследовательский Томский государственный университет» по специальности 10.05.01 Компьютерная безопасность (Утвержден Ученым советом НИ ТГУ, протокол от 30.06.2021 г. № 06).

Рабочая программа одобрена на заседании кафедры компьютерной безопасности

Протокол от 02 июня 2021 г. № 06

Заведующий кафедрой компьютерной безопасности,
канд. техн. наук, доцент С.А. Останин

Рабочая программа одобрена на заседании учебно-методической комиссии института прикладной математики и компьютерных наук (УМК ИПМКН)

Протокол от 17 июня 2021 г. № 05

Председатель УМК ИПМКН,
д-р техн. наук, профессор С.П. Сущенко

Цель освоения дисциплины

Цель – Обучить студентов алгоритмам над большими числами, над полиномами, методам генерации простых чисел, методам факторизации чисел и полиномов, задачам дискретного логарифмирования. Наряду с теоретическими основами, изучаются практические алгоритмы решения указанных задач. На лабораторных работах студенты реализуют, отлаживают и исследуют изучаемые алгоритмы. Именно это сочетание — теории и практики, математики и программирования — можно считать отличительной особенностью дисциплины.

1. Место дисциплины в структуре ОПОП

Дисциплина «Теоретико-числовые методы в криптографии» относится к части, формируемой участниками образовательных отношений Блока 1 «Дисциплины», входит в модуль «Специализация».

Пререквизиты дисциплины: Введение в математику, алгебра, теория чисел, языки программирования, методы программирования.

Постреквизиты дисциплины: Методы и средства криптографической защиты информации, Защита информации от утечки по техническим каналам.

2. Компетенции и результаты обучения, формируемые в результате освоения дисциплины

Таблица 1.

Компетенция	**Индикатор компетенции**	**Код и наименование результатов обучения** (планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций)
ОПК-3. Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности	ИОПК-3. Осуществляет применение основных понятий, фактов, концепций, принципов математики и информатики для решения задач профессиональной деятельности; ИОПК-3.3 Выявляет научную сущность проблем, возникающих в ходе профессиональной деятельности, и применяет соответствующий математический аппарат для их формализации, анализа и выработки решения.	ОР-3.1. Знать алгоритмы проверки чисел и многочленов на простоту, построения больших простых чисел, разложения чисел и многочленов на множители, дискретного логарифмирования в конечных циклических группах ОР-3.2. Владеть алгоритмами работы с большими числами, алгоритмами полиномиальной арифметики, методами решения теоретико- числовых задач в криптографии
ОПК-10 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности.	ИОПК-10.1 Осуществляет анализ тенденций развития методов и средств криптографической защиты информации.	ОР-10.1. Уметь применять математический аппарат алгебры и теории чисел для решения теоретико-числовых задач, возникающих в построении и анализе криптосистем ОР-10.2. Владеть навыками проведения компьютерных экспериментов над большими числами и полиномами
ПК-2 Способен проектировать и разрабатывать средства защиты информации компьютерных систем и сетей.	ИПК-2.1 Разрабатывает математические модели, реализуемые в средствах защиты информации.	ОР-2.1. Уметь создавать модели для исследования алгоритмов над большими числами, полиномами; алгоритмов генерации простых чисел, факторизации и дискретного логарифмирования ОР-2.2. Уметь использовать языки и системы

		программирования для реализации и исследования алгоритмов над большими числами, полиномами; алгоритмов генерации простых чисел, факторизации и дискретного логарифмирования

3. Структура и содержание дисциплины
3.1. Структура и трудоемкость видов учебной работы по дисциплине

Общая трудоемкость дисциплины составляет 9 зачетных единиц, 324 часа.

Таблица 2.

Вид учебной работы	Трудоемкость в академических часах		
	6 семестр	7 семестр	всего
Общая трудоемкость	144	180	324
Контактная работа:	71,5	71,5	143
Лекции (Л):	32	32	64
Практики (ПЗ)			
Лабораторные работы (ЛР)	32	32	64
Семинары (СЗ)			
Групповые консультации	2	2	4
Индивидуальные консультации	3,2	3,2	6,4
Промежуточная аттестация	2,3	2,3	4,6
Самостоятельная работа обучающегося:	76,8	40,8	117,6
- подготовка к рубежному контролю по теме/разделу	31,7	31,7	63,4
Вид промежуточной аттестации (зачет, зачет с оценкой, экзамен)	**Экзамен**	**Экзамен**	**Экзамен, экзамен**

3.2. Содержание и трудоемкость разделов дисциплины

Таблица 3.

Код занятия	Наименование разделов и тем и их содержание	Вид учебной работы, занятий, контроля	Семестр	Часы в электронной форме	Всего (час.)	Литература	Код (ы) результата(ов) обучения
	Раздел 1. Алгоритмы работы с большими числами		**6**				
1.1.	Дихотомический алгоритм возведения в степень	Лекции, лабораторные занятия, СРС	6		6	1, 2, 3, 4, 5, 6	ОР-3.1, ОР-3.3, ОР-10.1, ОР-10.2, ОР-2.1, ОР-2.2
1.2.	Метод Барретта	Лекции, лабораторные занятия, СРС	6		**6**	1, 2, 3, 4, 5, 6	ОР-3.1, ОР-3.3, ОР-10.1, ОР-10.2, ОР-2.1, ОР-2.2
1.3.	Преобразование Монтгомери	Лекции, лабораторные занятия, СРС	6		**6**	1, 2, 3, 4, 5, 6	ОР-3.1, ОР-3.3, ОР-10.1, ОР-10.2, ОР-2.1, ОР-2.2
1.4.	Теорема об извлечении корня	Лекции, лабораторные занятия, СРС	6		6	1, 2, 3, 4, 5, 6	ОР-3.1, ОР-3.3, ОР-10.1, ОР-10.2, ОР-2.1, ОР-2.2
1.5.	Вычисление НОД: бинарный алгоритм	Лекции, лабораторные занятия, СРС	6		7	1, 2, 3, 4, 5, 6	ОР-3.1, ОР-3.3, ОР-10.1, ОР-10.2, ОР-2.1, ОР-2.2
1.6.	Быстрое умножение: метод Карацубы, метод Тоома - Кука	Лекции, лабораторные занятия, СРС	6		7	1, 2, 3, 4, 5, 6	ОР-3.1, ОР-3.3, ОР-10.1, ОР-10.2, ОР-2.1, ОР-2.2
1.7.	Дискретное преобразование Фурье: определение, содержательный смысл	Лекции, лаборатор	6		7	1, 2, 3, 4, 5, 6	ОР-3.1, ОР-3.3, ОР-10.1, ОР-10.2, ОР-

		ные 7занятия, СРС					2.1, ОР-2.2
1.8.	Быстрое вычисление ДПФ	Лекции, лабораторные занятия, СРС	6		7	1, 2, 3, 4, 5, 6	ОР-3.1, ОР-3.3, ОР-10.1, ОР-10.2, ОР-2.1, ОР-2.2
1.9.	Алгоритм Шёнхаге - Штрассена умножения целых чисел	Лекции, лабораторные занятия, СРС	6		7	1, 2, 3, 4, 5, 6	ОР-3.1, ОР-3.3, ОР-10.1, ОР-10.2, ОР-2.1, ОР-2.2
	Раздел 2. Тесты на простоту и методы генерации простых чисел		**6**				
2.1.	Определение чисел Кармайкла. Теорема Кармайкла	Лекции, лабораторные занятия, СРС	6		7	1, 2, 3, 4, 5, 6	ОР-3.1, ОР-3.3, ОР-10.1, ОР-10.2, ОР-2.1, ОР-2.2
2.2.	Тест Соловея — Штрассена	Лекции, лабораторные занятия, СРС	6		7	1, 2, 3, 4, 5, 6	ОР-3.1, ОР-3.3, ОР-10.1, ОР-10.2, ОР-2.1, ОР-2.2
2.3.	Тест Миллера — Рабина	Лекции, лабораторные занятия, СРС	6		7	1, 2, 3, 4, 5, 6	ОР-3.1, ОР-3.3, ОР-10.1, ОР-10.2, ОР-2.1, ОР-2.2
2.4.	Метод Люка проверки числа на простоту	Лекции, лабораторные занятия, СРС	6		7	1, 2, 3, 4, 5, 6	ОР-3.1, ОР-3.3, ОР-10.1, ОР-10.2, ОР-2.1, ОР-2.2
2.5.	Простые числа специального вида: Ферма, Мерсенна, сильные простые, надёжные простые	Лекции, лабораторные занятия, СРС	6		7	1, 2, 3, 4, 5, 6	ОР-3.1, ОР-3.3, ОР-10.1, ОР-10.2, ОР-2.1, ОР-2.2
2.6.	Процедура генерации простого числа в Российском стандарте выработки ЭЦП	Лекции, лабораторные	6		7	1, 2, 3, 4, 5, 6	ОР-3.1, ОР-3.3, ОР-10.1, ОР-10.2, ОР-2.1, ОР-2.2

		занятия, СРС					
2.7.	Полиномиальный детерминированный тест на простоту	Лекции, лабораторные занятия, СРС	6		7	1, 2, 3, 4, 5, 6	ОР-3.1, ОР-3.3, ОР-10.1, ОР-10.2, ОР-2.1, ОР-2.2
	Раздел 3. Методы факторизации чисел		7				
3.1.	Факторизация: метод пробных делений	Лекции, лабораторные занятия, СРС	7		9	1, 2, 3, 4, 5, 6	ОР-3.1, ОР-3.3, ОР-10.1, ОР-10.2, ОР-2.1, ОР-2.2
3.2.	Факторизация: метод Олвея	Лекции, лабораторные занятия, СРС	7		9	1, 2, 3, 4, 5, 6	ОР-3.1, ОР-3.3, ОР-10.1, ОР-10.2, ОР-2.1, ОР-2.2
3.3.	Факторизация: метод Ферма	Лекции, лабораторные занятия, СРС	7		9	1, 2, 3, 4, 5, 6	ОР-3.1, ОР-3.3, ОР-10.1, ОР-10.2, ОР-2.1, ОР-2.2
3.4.	Факторизация: методы Полларда	Лекции, лабораторные занятия, СРС	7		9	1, 2, 3, 4, 5, 6	ОР-3.1, ОР-3.3, ОР-10.1, ОР-10.2, ОР-2.1, ОР-2.2
3.5.	Факторизация: метод Диксона	Лекции, лабораторные занятия, СРС	7		9	1, 2, 3, 4, 5, 6	ОР-3.1, ОР-3.3, ОР-10.1, ОР-10.2, ОР-2.1, ОР-2.2
3.6.	Факторизация: метод квадратичного решета	Лекции, лабораторные занятия, СРС	7		9	1, 2, 3, 4, 5, 6	ОР-3.1, ОР-3.3, ОР-10.1, ОР-10.2, ОР-2.1, ОР-2.2
3.7.	Факторизация: метод цепных дробей	Лекции, лабораторные занятия,	7		9	1, 2, 3, 4, 5, 6	ОР-3.1, ОР-3.3, ОР-10.1, ОР-10.2, ОР-2.1, ОР-2.2

		СРС					
3.8.	Алгоритм решета числового поля	Лекции, лабораторные занятия, СРС	7		9	1, 2, 3, 4, 5, 6	ОР-3.1, ОР-3.3, ОР-10.1, ОР-10.2, ОР-2.1, ОР-2.2
	Раздел 4. Дискретное логарифмирование не в конечных циклических группах		7				
4.1.	Дискретное логарифмирование: метод Полларда	Лекции, лабораторные занятия, СРС	7		9	1, 2, 3, 4, 5, 6	ОР-3.1, ОР-3.3, ОР-10.1, ОР-10.2, ОР-2.1, ОР-2.2
4.2.	Дискретное логарифмирование: алгоритм Адлемана	Лекции, лабораторные занятия, СРС	7		9	1, 2, 3, 4, 5, 6	ОР-3.1, ОР-3.3, ОР-10.1, ОР-10.2, ОР-2.1, ОР-2.2
4.3.	Дискретное логарифмирование: алгоритм Полита - Хеллмана	Лекции, лабораторные занятия, СРС	7		9	1, 2, 3, 4, 5, 6	ОР-3.1, ОР-3.3, ОР-10.1, ОР-10.2, ОР-2.1, ОР-2.2
	Раздел 5. Алгоритмы над полиномами: тесты на неприводимость, примитивность, факторизация полиномов		7				
5.1.	Критерии неприводимости многочленов по простому модулю	Лекции, лабораторные занятия, СРС	7		9	1, 2, 3, 4, 5, 6	ОР-3.1, ОР-3.3, ОР-10.1, ОР-10.2, ОР-2.1, ОР-2.2
5.2.	Тест на примитивность многочленов	Лекции, лабораторные занятия, СРС	7		9	1, 2, 3, 4, 5, 6	ОР-3.1, ОР-3.3, ОР-10.1, ОР-10.2, ОР-2.1, ОР-2.2
5.3.	Факторизация многочленов: освобождение от квадратов	Лекции, лабораторные занятия, СРС	7		9	1, 2, 3, 4, 5, 6	ОР-3.1, ОР-3.3, ОР-10.1, ОР-10.2, ОР-2.1, ОР-2.2
5.4.	Факторизация многочленов: алгоритм Берлекэмпа	Лекции, лаборатор	7		9	1, 2, 3, 4, 5, 6	ОР-3.1, ОР-3.3, ОР-10.1, ОР-10.2, ОР-

		ные занятия, СРС					2.1, ОР-2.2
5.5.	Метод Кантора — Цассенхауза	Лекции, лабораторные занятия, СРС	7		9	1, 2, 3, 4, 5, 6	ОР-3.1, ОР-3.3, ОР-10.1, ОР-10.2, ОР-2.1, ОР-2.2
	Подготовка к промежуточной аттестации в форме экзамена	СРС	**6**		**31,7**	1, 2, 3, 4, 5, 6	
	Прохождение промежуточной аттестации в форме экзамена	Э	**6**		**4,3**		
	…						
	Подготовка к промежуточной аттестации в форме экзамена	СРС	**7**		**31,7**	1, 2, 3, 4, 5, 6	
	Прохождение промежуточной аттестации в форме экзамена	Э	**7**		**4,3**		

4. Образовательные технологии, учебно-методическое и информационное обеспечение для освоения дисциплины

- для освоения дисциплины необходимо регулярное посещение лекций и повторение пройденного материала;
- самостоятельная работа студентов включает повторение пройденного материала и изучение рекомендованных разделов из основной и дополнительной литературы;
- промежуточная аттестация по дисциплине выполняется в виде контрольной работы по освоенному материалу.

Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения, характеризующих этапы формирования компетенций, и методические материалы, определяющие процедуры оценивания результатов обучения, приведены в Приложении 1 к рабочей программе «Фонд оценочных средств».

Типовые контрольные задания или иные материалы, необходимые для текущей аттестации, и методические материалы, определяющие процедуры оценивания результатов текущей аттестации, приведены в Приложении 2 к рабочей программе «Примерные оценочные средства текущей аттестации».

4.1. Рекомендуемая литература и учебно-методическое обеспечение

№ п/п	Авторы / составители	Заглавие	Издательство	Год издания, количество страниц
Основная литература				
1.	Ахо А.	Построение и анализ вычислительных алгоритмов	ЁЁ Медиа	2012 г., 534 с.
2.	Василенко О.Н.	Теоретико-числовые алгоритмы в криптографии	МЦНМО	2002 г.
3.	Кнут Д.	Искусство программирования для ЭВМ. Том 2. Получисленные алгоритмы	Мир	1977 г.
4.	Черёмушкин А.В.	Лекции по арифметическим алгоритмам в криптографии	МЦНМО	2002 г.
5.	Панкратова И.А.	Теоретико-числовые задачи в криптографии	РИО ТГУ	2010 г.
6.	Панкратова И.А.	Теоретико-числовые методы в криптографии	РИО ТГУ	2009 г.
Дополнительная литература				
7.	Фергюсон Н., Шнайер Б.	Практическая криптография	Диалектика	2005 г.
8.	Харин Ю.С., Берник В.И, Матвеев Г.В., Агиевин С.В.	атематические и компьютерные основы криптологии	Новое знание	2003 г.

4.2. Базы данных и информационно-справочные системы, в том числе зарубежные

1. Электронная библиотека (репозиторий) ТГУ [Электронный ресурс] / Электронная библиотека (репозиторий) ТГУ: [сайт]. – [Томск, 2011–2022]. – URL: http://vital.lib.tsu.ru/vital/access/manager/Index.

4.3. Перечень лицензионного и программного обеспечения

MS Windows; MS Office.

4.4. Оборудование и технические средства обучения

Для реализации дисциплины необходимы лекционные аудитории. Специальные технические средства (проектор, компьютер и т.д.) требуются для демонстрации материала в рамках изучаемых разделов, проведения защиты проектов в конце семестра. Вся основная и дополнительная литература, необходимая для самостоятельной работы и подготовки к экзамену, имеется в научной библиотеке ТГУ.

5. Методические указания обучающимся по освоению дисциплины

Обучающимся необходимо на лекциях строго фиксировать содержание излагаемого материала, перед каждой следующей лекцией освежать содержание предыдущей (при необходимости – предыдущих) лекции. В случае трудностей восприятия содержания – готовить вопросы преподавателю к очередной лекции.

6. Преподавательский состав, реализующий дисциплину

Останин Сергей Александрович, заведующий кафедрой компьютерной безопасности, канд. техн. наук, доцент.

Пахомова Елена Григорьевна, доцент кафедры компьютерной безопасности, канд. физ.-мат. наук, доцент.

7. Язык преподавания – русский язык.