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_» _июля_ 2021 г.

Фонд оценочных средств по дисциплине

Теоретико-числовые методы в криптографии

Специальность
10.05.01 Компьютерная безопасность
код и наименование специальности

Анализ безопасности компьютерных систем
наименование специализации

Томск–2021

ФОС 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

Фонд оценочных средств одобрен 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

Фонд оценочных средств (ФОС) является элементом системы оценивания сформированности компетенций у обучающихся в целом или на определенном этапе ее формирования.

ФОС разрабатывается в соответствии с рабочей программой (РП) дисциплины и включает в себя набор оценочных материалов для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине.

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

Компетенция	**Индикатор компетенции**	**Код и наименование результатов обучения** (планируемые результаты обучения, характеризующие этапы формирования компетенций)	**Критерии оценивания результатов обучения**			
			Отлично	Хорошо	Удовлетворительно	Неудовлетворительно
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	Уверенно владеет алгоритмами работы с большими числами, алгоритмами полиномиальной арифметики, методами решения теоретико-числовых задач в криптографии	Владеет алгоритмами работы с большими числами, алгоритмами полиномиальной арифметики, методами решения теоретико-числовых задач в криптографии	Знает основные понятия курса: алгоритмы проверки чисел и многочленов на простоту, построения больших простых чисел, разложения чисел и многочленов на множители, дискретного логарифмирования в конечных циклических группах	Не знает основные понятия курса: алгоритмы проверки чисел и многочленов на простоту, построения больших простых чисел, разложения чисел и многочленов на множители, дискретного логарифмирования в конечных циклических группах

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	Уверенно применяет математический аппарат алгебры и теории чисел для решения теоретико-числовых задач, возникающих в построении и анализе криптосистем	Хорошо умеет применять математический аппарат алгебры и теории чисел для решения теоретико-числовых задач, возникающих в построении и анализе криптосистем	Недостаточно умеет применять математический аппарат алгебры и теории чисел для решения теоретикочисловых задач, возникающих в построении и анализе криптосистем	Не умеет применять математический аппарат алгебры и теории чисел для решения теоретико-числовых задач, возникающих в построении и анализе криптосистем
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	Владеет навыками проведения компьютерных экспериментов над большими числами и полиномами	Умеет использовать языки и системы программирования для реализации и исследования алгоритмов над большими числами, полиномами; алгоритмов генерации простых	Умеет использовать языки и системы программирования для реализации алгоритмов над большими числами, полиномами	Не умеет использовать языки и системы программирования для реализации алгоритмов над большими числами, полиномами

2. Этапы формирования компетенций и виды оценочных средств

№	Этапы формирования компетенций (разделы дисциплины)	Код и наименование результатов обучения	Вид оценочного средства (тесты, задания, кейсы, вопросы и др.)
6 семестр			
1.	Алгоритмы работы с большими числами	ОР-3.1, ОР-3.3, ОР-10.1, ОР-10.2, ОР-2.1, ОР-2.2	Лабораторные работы, контрольные работы, экзамен
2.	Тесты на простоту и методы генерации простых чисел	ОР-3.1, ОР-3.3, ОР-10.1, ОР-10.2, ОР-2.1, ОР-2.2	Лабораторные работы, контрольные работы, экзамен
7 семестр			
1.	Методы факторизации чисел	ОР-3.1, ОР-3.3, ОР-10.1, ОР-10.2, ОР-2.1, ОР-2.2	Лабораторные работы, контрольные работы, экзамен
2.	Дискретное логарифмирование не в конечных циклических группах	ОР-3.1, ОР-3.3, ОР-10.1, ОР-10.2, ОР-2.1, ОР-2.2	Лабораторные работы, контрольные работы, экзамен
3.	Алгоритмы над полиномами: тесты на неприводимость, примитивность, факторизация полиномов	ОР-3.1, ОР-3.3, ОР-10.1, ОР-10.2, ОР-2.1, ОР-2.2	Лабораторные работы, контрольные работы, экзамен

3. Типовые контрольные задания или иные материалы, необходимые для оценки образовательных результатов обучения

3.1. Типовые задания для проведения текущего контроля успеваемости по дисциплине.

Темы лабораторных работ:

1. Алгоритмы возведения в степень
2. Методы приведения по модулю
3. Быстрые алгоритмы умножения чисел
4. Тесты на простоту: Ферма, Соловея — Штрассена, Миллера — Рабина
5. Методы генерации простых, надёжных простых и сильных простых чисел
6. Методы факторизации: пробных делений, Олвея, Ферма, решета, Полларда, методы случайных квадратов
7. Методы дискретного логарифмирования: Гельфонда, Полларда, Адлемана, Полита — Хеллмана
8. Проверка полиномов на неприводимость
9. Проверка полиномов на примитивность

Контрольные работы:

1. Методы умножения Карацубы и Тоома — Кука
2. Дискретное преобразование Фурье
3. Дискретное логарифмирование: методы Полита — Хеллмана, Полларда, Адлемана
4. Алгоритмы над полиномами: освобождение от квадратов, факторизация методом Берлекэмпа, проверта на примитивность

3.2. Типовые задания для проведения промежуточной аттестации по дисциплине.

Вопросы к экзамену

6 семестр

1. Дихотомический алгоритм возведения в степень

2. Алгоритм Барретта приведения чисел по модулю (с обоснованием)
3. Приведение по модулю специального вида
4. Преобразование Монтгомери
5. Произведение Монтгомери
6. Возведение в степень методом Монтгомери
7. Вычисление наибольшего общего делителя: бинарный алгоритм
8. Теорема о вычислении целой части квадратного корня
9. Быстрое умножение: метод Карацубы
10. Быстрое умножение: метод Тоома - Кука
11. Примитивные корни из 1, их свойства.
12. Теорема о матрице Вандермонда, её следствия
13. Теорема о примитивных корнях из 1
14. Дискретное преобразование Фурье: определение, содержательный смысл. Доказать обратимость ДПФ
15. Свертка. Теорема о свертке
16. Быстрое вычисление ДПФ: ключевые идеи
17. Алгоритм быстрого преобразования Фурье (с примером)
18. Определение чисел Кармайкла. Теорема Кармайкла
19. Определение и свойства оснований Ферма
20. Теорема о бесконечном количестве псевдопростых по любому основанию
21. Теорема о достаточности критерия Эйлера
22. Определение и свойства оснований Эйлера
23. Тест Соловея - Штрассена (с примером)
24. Теорема Селфриджа (о сильно псевдопростых числах)
2 5. Теорема Рабина
26. Тест Миллера - Рабина (с примером)
27. Пусть $n = 3 \pmod 4$. Доказать: R,, = E,,
28. Связь теста Миллера - Рабина с задачей факторизации
29. Метод Люка проверки числа на простоту (с примером)
30. Теорема Брилхарда — Лемера - Селфриджа (модификация критерия Люка)
31. Теорема Поклингтона, следствие её
32. Теорема Диемитко, следствие её
33. Процедура генерации простого числа в Российском стандарте выработки ЭЦП
34. Пусть $(a, n) = 1$. Доказать: n простое, если и только если $(x - a)^{n} = x^{n} — a \pmod n$
35. Полиномиальный детерминированный тест на простоту (AKS-тест)

7 семестр

1. Факторизация: метод пробных делений
2. Факторизация: метод Олвея
3. Факторизация: метод Ферма (с примером)
4. Факторизация: метод Ферма с просеиванием
5. Метод Флойда определения периода последовательности (с примером)
6. Факторизация: r-метод Полларда (с примером)
7. Факторизация: $(p - 1)$-метод Полларда (с примером)
8. Факторизация: метод Диксона (с примером)
9. Факторизация: метод квадратичного решета (с примером)
10. Метод квадратичного решета: этап просеивания (с примером)
11. Факторизация: метод цепных дробей (с примером)
12. Дискретное логарифмирование: r-метод Полларда (с примером)
13. Дискретное логарифмирование: алгоритм Адлемана (с примером)
14. Дискретное логарифмирование: алгоритм Полита - Хеллмана (с примером)
15. Критерии неприводимости многочленов по простому модулю
16. Тесты неприводимости многочленов (с примерами)

17. Тест на примитивность многочленов
18. Возвратные многочлены. Доказать: /(x) примитивный, если и только если/*(x) 19. примитивный
19. Факторизация многочленов: освобождение от квадратов
20. Теоремы Берлекэмла
21. Факторизация многочленов: алгоритм Берлекэмла
22. Метод Кантора — Цассенхауза: разложение полинома на делители с неприводимыми множителями одинаковой степени
23. Метод Кантора — Цассенхауза: второй этап, случай $p > 2$
24. Метод Кантора — Цассенхауза: второй этап, случай $p = 2$
25. Метод решета числового поля факторизации целых чисел (с примером для и [1] 65)

4. Методические материалы, определяющие процедуры оценивания образовательных результатов обучения

4.1. Методические материалы для оценки текущего контроля успеваемости по дисциплине.

В течение семестра необходимо выполнение всех обязательных практических заданий, лабораторных и контрольных работ.

4.2. Методические материалы для проведения промежуточной аттестации по дисциплине.

Промежуточная аттестация по дисциплине проводится в форме экзамена по теоретическому материалу.