МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ ТАДЖИКИСТАН
МЕЖГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКО-ТАДЖИКСКИЙ (СЛАВЯНСКИЙ) УНИВЕРСИТЕТ»

Естественнонаучный факультет

Кафедра «Информатики и ИТ»

«УТВЕРЖДАЮ»
«25» 10 2023 г.
Зав. кафедрой к.э.н., доцент
Лешукович А.И.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по

Математические основы защиты информации и информационной безопасности

09.04.03 «Прикладная информатика»

Душанбе 2023 г.

В результате освоения дисциплины «Математические основы защиты информации и информационной безопасности» формируются следующие (общепрофессиональные, профессиональные) компетенции обучающегося

Общепрофессиональные компетенции выпускников и индикаторы их достижения

1) Профессиональные компетенции: проектная деятельность:

Код	Формируемая компетенция	Содержание этапа формирования компетенции	Форма контроля
ПК-5	Способностью разрабатывать и адаптировать прикладное программное обеспечение.	**ИПК-5.1.** Применяет современные технологии разработки и адаптации прикладного программного обеспечения.	Тестирование. Контроль самостоятельной работы. Отчеты по практическим работам. Контрольная работа. Устный опрос.
		ИПК-5.2. Участвует в разработке на современных языках программирования и адаптации прикладного программного обеспечения	
		ИПК-5.3. Применяет современные технологии для разработки веб-приложений	

ПАСПОРТ
ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине Математические основы защиты информации и информационной безопасности

№ п/п	Контролируемые разделы, темы, модули[1]	Формируемые компетенции	Оценочные средства		
			Количество тестовых заданий	Другие оценочные средства	
				Вид	Количество
1	Примеры алгоритмов. Основные свойства интуитивного понятия алгоритма. Числовые функции: частичные, тотальные. Понятие интуитивно вычислимой функции и разрешимого множества. Необходимость математических моделей алгоритмов. Основные типы моделей алгоритмов.	ПК-5	6	Реферат	1
2	Машины Тьюринга как математическая модель алгоритма. Тезис Тьюринга. Вычисление функций на машинах Тьюринга. Построение машин Тьюринга. Тезисы Черча. Машина Поста.	ПК-5	8	Письменная работа	1

	Вычисление функций на машинах Поста. Построение машин Поста.				
3	Базисные функции: нулевая, следования, проекции. Операторы суперпозиции и примитивной рекурсии. Примитивно-рекурсивные функции. Оператор минимизации. Частично-рекурсивные функции. Тотально-рекурсивные функции. Примеры примитивно (частично, тотально)-рекурсивных функций. Тезис Черча.	ПК-5	10	Контрольная работа	1
4	Нормальные алгорифмы Маркова как математическая модель алгоритма. Принцип нормализации Маркова. Вычисление функций нормальными алгорифмами. Доказательство равнообъемности математических моделей алгоритмов: машин Тьюринга, частично-рекурсивных функций.	ПК-5	18	Контрольная работа	1
5	Характеристическая функция множества. Определение рекурсивных и перечислимых множеств. Перечислимость рекурсивных множеств. Критерий рекурсивности.	ПК-5	12	Контрольная работа	1
6	Кодирование машин Тьюринга. универсальная машина Тьюринга. Перечислимость множества частично-рекурсивных функций. Универсальная частично-рекурсивная функция. Существование универсальной функции для множества n-местных частично-рекурсивных функций.	ПК-5	8	Контрольная работа	1
7	Массовые алгоритмические проблемы. Неразрешимость проблемы остановки машин Тьюринга. Алгоритмическая сводимость. Обзор алгоритмически неразрешимых проблем	ПК-5	12	Контрольная работа	1
8	Сортировка и определение сложности алгоритмов сортировки. Сортировка вставками. Пузырьковая сортировка. Сортировка выбором. Быстрая сортировка. Сортировка слиянием. Пирамидальная сортировка. Сортировка перечислением. Сортировка всплытием. Сортировка бинарным поиском. Алгоритмы сортировки, использую-	ПК-5	8	Контрольная работа	1

	щие структуру элементов: цифровая сортировка, корневая сортировка				

ТЕМЫ РЕФЕРАТОВ И ПИСЬМЕННЫХ РАБОТ
(рефератов, эссе, письменных работ)

1. Алгебраические структуры: группы, кольца, поля. Теорема Лагранжа о порядке элемента группы.
2. Конечные поля. Расширения конечных полей. Вычисление обратных элементов в поле.
3. Модулярная арифметика. Решение сравнений 1 порядка.
4. Символ Лежандра. Его свойства и вычисление.
5. Производящие функции числовых последовательностей. Определение и основные свойства. Примеры.
6. Дифференцирование и интегрирование производящих функций.
7. Таблица производящих функций.
8. Вычисление производящей функции ряда Фибоначчи.
9. Полные и приведенные системы вычетов в кольце Z_n.
10. Мультипликативные функции. Функция Эйлера. Формула для вычисления функции Эйлера. Теорема Эйлера о порядке элемента в Z_n.
11. Функция Мебиуса. Теорема о сумме значений функции Мебиуса по всем делителям натурального числа n
12. Формула инверсии Мебиуса. Формула включений/исключений. Ее использование для вычисления функции простых чисел $\pi(x)$.
13. Функция Мангольда и ее свойства. Функция деления.
14. Произведение (конволюция) Дирихле. Мультипликативность конволюции мультипликативных функций.
15. Инверсия Дирихле. Теорема об инверсии Дирихле мультипликативной функции.
16. Ряды Дирихле. Дзета-функция Римана. Произведение рядов Дирихле.
17. Теорема Эйлера о сумме ряда обратных квадратов
18. Свойства дзета-функции Римана. Формула произведения Эйлера
19. Формула суммирования Эйлера-Маклорена (без доказательства).
20. Нахождение асимптотической формулы для частичной суммы гармонического ряда и ряда обратных квадратов.
21. Формулы Стирлинга и ее вывод с помощью формулы суммирования Эйлера-Маклорена.
22. Гладкие и гладкостепенные числа. Формула Бухштаба вычисление числа y-гладких чисел.
23. Факторизация натуральных чисел. Метод Ленстры факторизации на эллиптических кривых.
24. Анализ сходимости метода факторизации Ленстры с помощью изучения распределения гладко-степенных чисел.
25. Метод квадратичного решета факторизации натуральных чисел. Основные параметры метода и их выбор.

Критерии оценки выполнения самостоятельной работы.

В основу разработки балльно рейтинговой системы положены принципы, в соответствии с которыми формирование рейтинга студента осуществляется постоянно в процессе его обучения в университете. Настоящая система оценки успеваемости студентов основана на использовании совокупности контрольных точек, равномерно расположенных на всем временном интервале изучения дисциплины. При этом предполагается разделение всего курса на ряд более или менее самостоятельных, логически завершенных блоков и модулей и проведение по ним промежуточного контроля.

Студентам выставляются следующие баллы за выполнение задания к ПК:

- оценка «отлично» (10 баллов): контрольные тесты, а также самостоятельно выполненные семестровые задания, выполненные полностью и сданные в срок в соответствии с предъявляемыми требованиями;

- оценка «хорошо» (8-9 баллов): задание выполнено и в целом отвечает предъявляемым требованиям, но имеются отдельные замечания в его оформлении или сроке сдачи;

- оценка «удовлетворительно» (6-7 баллов): задание выполнено не до конца, отсутствуют ответы на отдельные вопросы, имеются отклонения в объеме, содержании, сроке выполнения;

- оценка «неудовлетворительно» (5 и ниже): отсутствует решение задачи, задание переписано (скачано) из других источников, не проявлена самостоятельность при его выполнении.

Текущий контроль осуществляется в ходе учебного процесса по результатам выполнения самостоятельной работы и контрольной работы.

Основными формами текущего контроля знаний являются:

- обсуждение вынесенных в планах практических занятий лекционного материала и контрольных вопросов;
- решение тестов и их обсуждение с точки зрения умения сформулировать выводы, вносить рекомендации и принимать адекватные управленческие решения;
- выполнение контрольной работы и обсуждение результатов;
- участие в дискуссиях в качестве участника и модератора групповой дискуссии по темам дисциплины;
- написание и презентация доклада;
- написание самостоятельной (контрольной) работы.

Для контроля усвоения данной дисциплины учебным планом предусмотрен экзамен. Общее количество баллов по дисциплине - 100 баллов. Распределение баллов на текущий и промежуточный контроль при освоении дисциплины, а также итоговой оценке представлено ниже.

КОНТРОЛЬНЫЕ ЗАДАНИЯ И ВОПРОСЫ ДЛЯ ТЕКУЩЕГО

КОНТРОЛЯ ЗНАНИЙ ПО ДИСЦИПЛИНЕ

(ДЛЯ ТЕКУЩЕЙ АТТЕСТАЦИИ И КОНТРОЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ)

24. Мультипликативные функции. Функция Эйлера. Формула для вычисления функции Эйлера.Теорема Эйлера о порядке элемента в Z_n.

25. Функция Мебиуса. Теорема о сумме значений функции Мебиуса по всем делителям натурального числа n

26. Формула инверсии Мебиуса. Формула включений/исключений. Ее использование для вычисления функции простых чисел $\pi(x)$.

27. Функция Мангольда и ее свойства. Функция деления.

28. Произведение (конволюция) Дирихле. Мультипликативность конволюции мультипликативных функций.

29. Инверсия Дирихле. Теорема об инверсии Дирихле мультипликативной функции.

30. Ряды Дирихле. Дзета-функция Римана. Произведение рядов Дирихле.

31. Теорема Эйлера о сумме ряда обратных квадратов

32. Свойства дзета-функции Римана. Формула произведения Эйлера

33. Формула суммирования Эйлера-Маклорена (без доказательства).

34. Нахождение асимптотической формулы для частичной суммы гармонического ряда и ряда обратных квадратов.

35. Формулы Стирлинга и ее вывод с помощью формулы суммирования Эйлера-Маклорена.

Итоговые оценки студентов

Буквенное обозначение итоговых оценок студентов и их цифровые эквиваленты:

Буквенная оценка	Цифра	Общий балл	Традиционная оценка
A	4	95≤A≤100	отлично
A-	3,67	90≤A-<95	
B+	3,33	85≤B+<90	хорошо
B	3	80≤B<85	
B-	2,67	75≤B-<80	
C+	2,33	70≤C+<75	удовлетворительно

C	2	65≤C<70	
C-	1,67	60≤C-<65	
D+	1,33	55≤D+<60	
D	1	50≤D<55	
Fx	0	45≤Fx<50	неудовлетворительно
F	0	0<F<45	

Критерии выведения итоговой оценки промежуточной аттестации:

«Отлично» - средняя оценка ≥ 3,67.
«Хорошо» - средняя оценка ≥ 2,67 и ≤ 3,33.
«Удовлетворительно» - средняя оценка ≥ 1,0 и ≤ 2,33.
«Неудовлетворительно» - средняя оценка < 0.