

МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Санкт-Петербургский государственный экономический университет»

УТВЕРЖДАЮ

Проректор по учебной и
методической работе

_____ В.Г. Шубаева

« ____ » _____ 20 ____ г.

ДИСКРЕТНАЯ МАТЕМАТИКА

Рабочая программа дисциплины

Направление подготовки 10.03.01 Информационная безопасность

Направленность
(профиль) программы

Безопасность компьютерных систем
(в экономике и управлении)

Уровень высшего
образования

Бакалавриат

Форма обучения очная

Составитель:

_____ / к.ф.-м.н., доц. Десницкая В. Н.

Санкт-Петербург
2020

СОДЕРЖАНИЕ

1. ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ.....	4
2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП	Ошибка! Закладка не определена.
3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ	Ошибка! Закладка не определена.
4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ	4
5. СОДЕРЖАНИЕ РАЗДЕЛОВ И ТЕМ ДИСЦИПЛИНЫ.....	5
6. ЗАНЯТИЯ СЕМИНАРСКОГО ТИПА.....	6
7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ	7
8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ.....	Ошибка! Закладка не определена.
9. РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ.	Ошибка! Закладка не определена.
9.1. Учебно-методическое и информационное обеспечение дисциплины	Ошибка! Закладка не определена.
9.2. Материально-техническое обеспечение учебного процесса	9
10. ОСОБЕННОСТИ ОСВОЕНИЯ ДИСЦИПЛИНЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ.....	Ошибка! Закладка не определена.
11. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ	Ошибка! Закладка не определена.
12. ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ.....	10

1. ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ

Цель дисциплины: дать обучающимся необходимый запас сведений по ряду разделов дискретной математики (основные определения, теоремы, правила), наиболее соответствующих их будущей профессиональной деятельности, а также математический аппарат, помогающий им ставить в математической форме и решать профессиональные задачи.

Задачи дисциплины: познакомить обучающихся с математическими понятиями и методами дискретной математики, используемыми в информатике, в частности в защите информации; способствовать развитию логического, математического и алгоритмического мышления, способствовать формированию умений и навыков самостоятельного анализа и исследования профессиональных проблем, развитию стремления к научному поиску путей совершенствования своей работы.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина Б1.Б.13 «Дискретная математика» относится к базовой части Блока 1 РУП ОПОП, и является обязательной для освоения обучающимся вне зависимости от направленности (профиля) программы.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения ОПОП, представлены в таблице 3.1.

Таблица 3.1 – Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения ОПОП

Код и наименование компетенции выпускника	Уровень освоения компетенции	Планируемые результаты обучения (показатели освоения компетенции)
ОПК-3 – Способен работать с компьютером как средством управления информацией из различных источников, в том числе в глобальных компьютерных сетях	Третий уровень (продвинутый) (ОПК-3) –3	Знать: основные положения дискретной математики: элементы теории множеств, элементы теории чисел, теории кодирования ЗЗ (ОПК-3) Уметь: использовать математические методы и модели для решения прикладных задач дискретной математики УЗ (ОПК-3) Владеть: навыками моделирования и решения прикладных задач методами дискретной математики ВЗ (ОПК-3)

4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ

Трудоемкость дисциплины составляет 3 зачетные единицы, 108 часов, из которых 36 часов самостоятельной работы студента согласно РУП отводится на подготовку и защиту экзамена.

Форма промежуточной аттестации: экзамен - 4 семестр.

Распределение фонда времени по темам дисциплины по очной форме обучения представлено в таблице 4.1.

Таблица 4.1 – Распределение фонда времени по темам дисциплины (очная форма обучения)

Номер и наименование тем	Объем дисциплины (ак. часы)				Формы текущего контроля успеваемости
	Контактная работа			СРО	
	ЗЛТ	ПЗ	ЛР		
1	2	3	4	5	6
Тема 1. Множества и операции над ними. Отображения, их свойства. Сравнение множеств	2	2		4	Рубежный контроль
Тема 2. Бинарные отношения. Отношения эквивалентности и порядка	2	2		4	Рубежный контроль
Тема 3. Делимость чисел. Деление с остатком. Наибольший общий делитель. Алгоритм Евклида.	2	2		4	Рубежный контроль
Тема 4. Решение неопределенных уравнений при помощи алгоритма Евклида.	2	2		4	Рубежный контроль
Тема 5. Модулярная арифметика.	2	4		6	Рубежный контроль
Тема 6. Простые числа. Функция Эйлера. Теоремы Эйлера и Ферма	2	4		6	Рубежный контроль
Тема 7. Решение сравнений первой степени. Системы сравнений	4	4		8	Рубежный контроль
Тема 8. Цепные дроби. Подходящие дроби, их свойства и применение	2	6		8	Рубежный контроль
Тема 9. Квадратичные вычеты. Проверка чисел на простоту	2	4		6	Рубежный контроль
Тема 10. Теория чисел в криптографии	2	2		4	Рубежный контроль
Всего за семестр:	22	32		54	Экзамен
Всего по дисциплине:	22	32		54	Экзамен

5. СОДЕРЖАНИЕ РАЗДЕЛОВ И ТЕМ ДИСЦИПЛИНЫ

Основные структуры

Тема 1. Множества и операции над ними. Отображения, их свойства. Сравнение множеств.

Множества и способы их задания. Числовые множества. Алгебра множеств. Отображения, их свойства. Мощность множества.

Тема 2. Бинарные отношения. Отношения эквивалентности и порядка.

Бинарные отношения, их свойства. Отношение эквивалентности. Классы эквивалентности, фактор-множество. Отношение порядка. Порядок по Парето. Лексикографический порядок.

Тема 3. Делимость чисел. Деление с остатком. Наибольший общий делитель. Алгоритм Евклида.

Делимость чисел, свойства делимости. Деление с остатком. Наибольший общий делитель, его свойства. Вычисление наибольшего общего делителя при помощи алгоритма Евклида.

Тема 4. Решение неопределенных уравнений при помощи алгоритма Евклида.

Взаимно простые числа. Решение неопределенных уравнений при помощи алгоритма Евклида.

Тема 5. Модулярная арифметика

Сравнения по модулю, их свойства. Нахождение остатков от деления при помощи свойств сравнения по модулю.

Тема 6. Простые числа. Функция Эйлера. Теоремы Эйлера и Ферма.

Простое число. Каноническое разложение числа. Функция Эйлера, ее свойства. Теорема Эйлера, теорема Ферма. Нахождение остатков от деления при помощи теорем Эйлера и Ферма.

Тема 7. Решение сравнений первой степени. Системы сравнений

Решение сравнений при помощи алгоритма Евклида и при помощи теоремы Эйлера. Системы сравнений. Китайская теорема об остатках.

Тема 8. Цепные дроби. Подходящие дроби, их свойства и применение

Представление рациональных чисел цепными дробями. Подходящие дроби, их свойства. Решение неопределенных уравнений при помощи подходящих дробей. Представление иррациональных чисел цепными дробями.

Тема 9. Квадратичные вычеты. Проверка чисел на простоту

Квадратичные вычеты и невычеты. Символ Лежандра, его свойства и применение. Квадратичный закон взаимности Гаусса. Символ Якоби, его свойства и применение. Алгоритмы проверки чисел на простоту. Вероятностный тест Соловея-Штрассена.

Тема 10. Теория чисел в криптографии

Задача шифрования. Использование теории чисел в шифровании. Шифр RSA, его обоснование.

6. ЗАНЯТИЯ СЕМИНАРСКОГО ТИПА

Таблица 6.1 – Практические занятия/ Семинарские занятия / Лабораторные работы

№ темы	Тема занятия	Вид занятия
--------	--------------	-------------

1	2	3
	3 семестр	
1	ПЗ.1. Теоретико-множественные операции. Декартово произведение множеств. Отображения, функции. Метод математической индукции.	ПЗ/Решение практических задач
2	ПЗ.2. Бинарные отношения, их свойства. Отношение эквивалентности. Лексикографический порядок и порядок по Парето.	ПЗ/Решение практических задач
3	ПЗ.3. Нахождение наибольшего общего делителя чисел при помощи алгоритма Евклида. Решение неопределенных уравнений.	ПЗ/Решение практических задач
4	ПЗ.4. Решение неопределенных уравнений при помощи алгоритма Евклида.	ПЗ/Решение практических задач
5	ПЗ.5. Свойства сравнения по модулю. ПЗ.6. Нахождение остатков от деления при помощи свойств сравнения по модулю.	ПЗ/Решение практических задач
6	ПЗ.7. Простые числа. Каноническое разложение чисел. Вычисление функции Эйлера. ПЗ.8. Нахождение остатков от деления при помощи теорем Эйлера и Ферма.	ПЗ/Решение практических задач
7	ПЗ.9. Решение сравнений первой степени. ПЗ.10. Решение систем сравнений первой степени. Китайская теорема об остатках.	ПЗ/Решение практических задач
8	ПЗ.11. Представление рациональных чисел цепными дробями. Подходящие дроби. ПЗ.12. Решение неопределенных уравнений при помощи подходящих дробей. ПЗ.13. Представление иррациональных чисел цепными дробями.	ПЗ/Решение практических задач
9	ПЗ.14. Квадратичные вычеты. Символ Лежандра, его свойства и применение. Квадратичный закон взаимности Гаусса. ПЗ.15. Символ Якоби, его свойства и применение. Тесты проверки чисел на простоту.	ПЗ/Решение практических задач
10	ПЗ.16. Шифр RSA.	ПЗ/Решение практических задач

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ

7.1. Методические указания для обучающегося по освоению дисциплины

Для формирования четкого представления об объеме и характере знаний и умений, которыми надо будет овладеть по дисциплине в самом начале учебного курса обучающийся должен ознакомиться с учебно-методической документацией:

- рабочей программой дисциплины: с целями и задачами дисциплины, ее связями с другими дисциплинами образовательной программы, перечнем знаний и умений, которыми в процессе освоения дисциплины должен владеть обучающийся,

– порядком проведения текущего контроля успеваемости и промежуточной аттестации;

– графиком консультаций преподавателей кафедры.

Систематическое выполнение учебной работы на занятиях лекционных и семинарских типов, а также выполнение самостоятельной работы позволит успешно освоить дисциплину.

В процессе освоения дисциплины обучающимся следует:

- слушать, конспектировать излагаемый преподавателем материал;
- ставить, обсуждать актуальные проблемы курса, быть активным на занятиях;
- задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений;
- выполнять задания практических занятий полностью и установленные сроки.

При затруднениях в восприятии материала следует обратиться к основным литературным источникам. Если разобраться в материале не удалось, то обратиться к лектору (по графику его консультаций) или к преподавателю на занятиях семинарского типа.

Обучающимся, пропустившим занятия (независимо от причин), не имеющим письменного решения задач или не подготовившимся к данному занятию, рекомендуется не позже чем в 2 - недельный срок явиться на консультацию к преподавателю и отчитаться по теме.

7.2. Организация самостоятельной работы

Под самостоятельной работой обучающихся понимается планируемая работа обучающихся, направленная на формирование указанных компетенций, выполняемая во внеаудиторное время по заданию и при методическом руководстве преподавателя, без его непосредственного участия.

Методическое обеспечение самостоятельной работы при наличии обучающихся лиц с ограниченными возможностями представляется в формах, адаптированных к ограничениям их здоровья.

Виды самостоятельной работы по дисциплине представлены в таблице 7.2.1.

Таблица 7.2.1 – Организация самостоятельной работы обучающегося

№ тем ы	Вид самостоятельной работы
1	2
1 - 6	Изучение теоретических вопросов курса, подготовка к практическим занятиям, подготовка к тестированию (контрольным работам) №1. Подготовка к экзамену.
7-11	Изучение теоретических вопросов курса, подготовка к практическим занятиям, подготовка к тестированию (контрольным работам) №2. Подготовка к экзамену

Каждый вид СРО, указанный в таблице 7.2.1 обеспечен методическими материалами.

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В преподавании дисциплины «Дискретная математика» в основном используются традиционные методы обучения. При изложении отдельных тем применяются активные и интерактивные технологии (лекции-визуализации, групповое решение задач на практическом занятии, интерактивная работа в малых группах).

9. РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

9.1. Учебно-методическое и информационное обеспечение дисциплины

Таблица 9.1.1 – Учебно-методическое и информационное обеспечение дисциплины

Наименование литературы: автор, название, издательство	Год	КНИГООБЕСПЕЧЕННОСТЬ	
		Печатные издания (кол-во экземпляров)	Электронные (наименование ресурсов)
1	2	3	4

9.2. Материально-техническое обеспечение учебного процесса

Для реализации данной дисциплины имеются специальные помещения для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы.

Таблица 9.2.1 – Материально-техническое обеспечение дисциплины

Вид учебных занятий по дисциплине	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
1	2
Лекции	Программное обеспечение не предусмотрено
Практические занятия	Программное обеспечение не предусмотрено

10. ОСОБЕННОСТИ ОСВОЕНИЯ ДИСЦИПЛИНЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Обучение обучающихся с ограниченными возможностями здоровья при необходимости осуществляется на основе адаптированной рабочей программы с использованием специальных методов обучения и дидактических материалов, составленных с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся (обучающегося).

В целях освоения учебной программы дисциплины инвалидами и лицами с ограниченными возможностями здоровья Университет обеспечивает:

– для инвалидов и лиц с ограниченными возможностями здоровья по зрению: размещение в доступных для обучающихся, являющихся слепыми или слабовидящими, местах и в адаптированной форме справочной информации о расписании учебных занятий; присутствие ассистента, оказывающего обучающемуся необходимую помощь;

выпуск альтернативных форматов методических материалов (крупный шрифт или аудиофайлы);

- для инвалидов и лиц с ограниченными возможностями здоровья по слуху: надлежащими звуковыми средствами воспроизведение информации;

- для инвалидов и лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата: возможность беспрепятственного доступа обучающихся в учебные помещения, туалетные комнаты и другие помещения кафедры, а также пребывание в указанных помещениях.

Образование обучающихся с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах или в отдельных организациях.

11. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Фонд оценочных средств для проведения аттестации уровня сформированности компетенций обучающихся по дисциплине оформляется отдельным документом и является приложением к рабочей программе дисциплины (модуля).

12. ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

в рабочую программу дисциплины « Дискретная математика»
образовательной программы направления подготовки 38.03.05 Бизнес-
информатика, направленность: Деловая аналитика

[illegible]

