Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Национальный исследовательский университет «МЭИ»

Направление подготовки/специальность: 10.03.01 Информационная безопасность

Наименование образовательной программы: Организация и технология защиты информации

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

Рабочая программа дисциплины
ДИСКРЕТНАЯ МАТЕМАТИКА-2

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Вариативная**
№ дисциплины по учебному плану:	**Б1.В.09.02.02**
Трудоемкость в зачетных единицах:	**5 семестр - 5;**
Часов (всего) по учебному плану:	**180 часов**
Лекции	**5 семестр - 32 часа;**
Практические занятия	**5 семестр - 32 часа;**
Лабораторные работы	**5 семестр - 16 часов;**
Консультации	**5 семестр - 2 часа;**
Самостоятельная работа	**5 семестр - 97,5 часа;**
в том числе на КП/КР	**не предусмотрено учебным планом**
Иная контактная работа	**проводится в рамках часов аудиторных занятий**
включая: **Контрольная работа**	
Промежуточная аттестация:	
Экзамен	**5 семестр - 0,5 часа;**

Москва 2019

ПРОГРАММУ СОСТАВИЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Евтеев Б.В. Идентификатор: Rbb7ca24a-YevteevBV-e22a6fbb	Б.В. Евтеев
(должность)	(подпись)	(расшифровка подписи)

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Баронов О.Р. Идентификатор: R90d76356-BaronovOR-7bf8fd7e	О.Р. Баронов
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)
Заведующий выпускающей кафедры	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d	А.Ю. Невский
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины: Цель освоения дисциплины сформировать систему знаний и навыков по применению дискретных математических моделей для обеспечения информационной безопасности

Задачи дисциплины

- −изучение аппарата теории булевых функций и их криптографических свойств для обеспечения информационной безопасности;
- -изучение комбинаторных методов дискретной математики для их использования при решении задач защиты информации;
- -изучение алгоритмов на графах;
- - изучение алгебраических структур и модулярной арифметики.

Формируемые у обучающегося **компетенции** и запланированные **результаты обучения** по дисциплине, соотнесенные с **индикаторами достижения компетенций**:

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Запланированные результаты обучения**
ОПК-2 способностью применять соответствующий математический аппарат для решения профессиональных задач		знать: - теорию булевых функций и алгебраических структур; - комбинаторные методы, теорию графов. уметь: - анализировать свойства булевых функций и использовать булевы функции с требуемыми свойствами; - применять методы дискретной математики при решении прикладных задач.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к части, формируемой участниками образовательных отношений блока дисциплин основной профессиональной образовательной программе Организация и технология защиты информации (далее – ОПОП), направления подготовки 10.03.01 Информационная безопасность, уровень образования: высшее образование - бакалавриат.

Базируется на уровне среднего общего образования.

Результаты обучения, полученные при освоении дисциплины, необходимы при выполнении выпускной квалификационной работы.

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 5 зачетных единиц, 180 часов.

№ п/п	Разделы/темы дисциплины/формы промежуточной аттестации	Всего часов на раздел	Семестр	Распределение трудоемкости раздела (в часах) по видам учебной работы										Содержание самостоятельной работы/ методические указания
				Контактная работа								СР		
				Лек	Лаб	Пр	Консультация		ИКР		ПА	Работа в семестре	Подготовка к аттестации /контроль	
							КПР	ГК	ИККП	ТК				
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	Булевы функции и их криптографические свойства	38	5	8	4	8	-	-	-	-	-	18	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Булевы функции и их криптографические свойства"
1.1	Булевы функции	19		4	2	4	-	-	-	-	-	9	-	***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы
1.2	Криптографические свойства булевых функций	19		4	2	4	-	-	-	-	-	9	-	***Подготовка к контрольной работе:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Булевы функции и их криптографические свойства" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Булевы функции и их криптографические свойства" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Булевы функции и их криптографические свойства"

														Изучение материалов литературных источников: [1], Гл.2, Гл.14 [2], Гл.1 [4], Гл.6, Гл.7 [5], Гл.4
2	Комбинаторные методы	44		10	4	10	-	-	-	-	-	20	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Комбинаторные методы" ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Комбинаторные методы" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. ***Подготовка к контрольной работе:*** Изучение материалов по разделу Комбинаторные методы и подготовка к контрольной работе ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Комбинаторные методы" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Комбинаторные методы" ***Изучение материалов литературных источников:*** [1], Гл.5
2.1	Общая комбинаторная схема	10		2	-	2	-	-	-	-	-	6	-	
2.2	Рекуррентные соотношения и производящие функции	16		4	2	4	-	-	-	-	-	6	-	
2.3	Классификация булевых функций	18		4	2	4	-	-	-	-	-	8	-	

														[2], Гл.8 [3], Ч.2 [5], Гл.2
3	Графы	33		8	4	8	-	-	-	-	-	13	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Графы и преобразования" ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Графы и преобразования" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. ***Подготовка к контрольной работе:*** Изучение материалов по разделу Графы и преобразования и подготовка к контрольной работе ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Графы и преобразования" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Графы и преобразования" ***Изучение материалов литературных источников:*** [1], Гл.6 [2], Гл.4 [3], Ч.4 [5], Гл.3
3.1	Элементы теории графов	16		4	2	4	-	-	-	-	-	6	-	
3.2	Графы преобразований и их свойства	17		4	2	4	-	-	-	-	-	7	-	
4	Алгебраические	29		6	4	6	-	-	-	-	-	13	-	***Подготовка к текущему контролю:***

	структуры и основы модулярной арифметики													Повторение материала по разделу "Алгебраические структуры и основы модулярной арифметики"
4.1	Алгебраические основы	12		2	2	2	-	-	-	-	-	6	-	***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы
4.2	Теоретико-числовые основы	17		4	2	4	-	-	-	-	-	7	-	***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Алгебраические структуры и основы модулярной арифметики" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. ***Подготовка к контрольной работе:*** Изучение материалов по разделу Алгебраические структуры и основы модулярной арифметики и подготовка к контрольной работе ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Алгебраические структуры и основы модулярной арифметики" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Алгебраические структуры и основы модулярной арифметики" ***Изучение материалов литературных источников:*** [2], Гл.2 [3], Гл.2 [4], Гл.4 [5], Гл 1

														[6], Ч. 1
	Экзамен	36.0		-	-	-	-	2	-	-	0.5	-	33.5	
	Всего за семестр	**180.0**		**32**	**16**	**32**	**-**	**2**	**-**	**-**	**0.5**	**64**	**33.5**	
	Итого за семестр	**180.0**		**32**	**16**	**32**	**2**		**-**		**0.5**	**97.5**		

Примечание: Лек – лекции; Лаб – лабораторные работы; Пр – практические занятия; КПР – аудиторные консультации по курсовым проектам/работам; ИККП – индивидуальные консультации по курсовым проектам/работам; ГК- групповые консультации по разделам дисциплины; СР – самостоятельная работа студента; ИКР – иная контактная работа; ТК – текущий контроль; ПА – промежуточная аттестация

3.2 Краткое содержание разделов

1. Булевы функции и их криптографические свойства

1.1. Булевы функции

Представления булевых функций, полиномы Жегалкина, быстрое преобразование Мёбиуса. Числовые и метрические характеристики. Спектральное представление булевых функций: спектр Фурье и Уолша-Адамара. Взаимосвязь различных представлений булевых функций Нелинейность булевых функций.

1.2. Криптографические свойства булевых функций

Уравновешенное отображение. Нелинейность криптографических отображений. Бент-функции Корреляционно-иммунные и устойчивые функции. Устойчивые отображения. Линейные структуры отображений и индекс линейности отображения..

2. Комбинаторные методы

2.1. Общая комбинаторная схема

Распределение шаров по ящикам. Числа Стирлинга второго рода. Подсчет количества разбиений и разложений чисел..

2.2. Рекуррентные соотношения и производящие функции

Однородные рекуррентные соотношения. Неоднородные рекуррентные соотношения. Метод производящих функций. Числа Фибоначчи..

2.3. Классификация булевых функций

Групповая эквивалентность отображений. Теория перечисления Пойа и классификация булевых функций..

3. Графы

3.1. Элементы теории графов

Способы задания графов. Полные графы. Двудольные графы. Подграфы. Минимальное остовное дерево. Изоморфизм графов. Раскраска графа. Циклы и разрезы в графе. Эйлеровы и гамильтоновы графы. Оптимизационные алгоритмы на графах..

3.2. Графы преобразований и их свойства

Группы подстановок и представление их элементов в виде произведения независимых циклов. Числа Стирлинга первого рода. Характеристики периодичности преобразований, полноцикловые преобразования.

4. Алгебраические структуры и основы модулярной арифметики

4.1. Алгебраические основы

Бинарные операции на множестве. Примеры бинарных операций и виды алгебраических структур: полугруппы, моноиды, группы. Гомоморфизмы и изоморфизмы групп. Подгруппы. Смежные классы группы по подгруппе. Теорема Лагранжа. Нормальные делители. Фактор - группы. Теорема о гомоморфизмах. Прямые произведения групп и подгрупп. Группы подстановок. Теорема Кэли. Теорема Бернсайда. Кольца и поля.

4.2. Теоретико-числовые основы

Делимость чисел. Алгоритм Евклида. Факторизация числа. Сравнимость чисел. Классы вычетов. Таблица сложения и умножения по модулю p и m. Обратимые элементы по модулю m. Решение сравнений первой степени. Решение систем линейных уравнений в поле вычетов по модулю. Китайская теорема об остатках. Решение систем сравнений. Функция Эйлера. Теорема Эйлера. Решение задач факторизации и дискретного логарифмирования.

3.3. Темы практических занятий

1. 3.Криптографические свойства булевых функций;
2. 4.Линейные рекуррентные соотношения;
3. 5.Метод производящих функций;
4. 6.Матрицы смежности, инцидентности, весов и расстояний графов;
5. 7.Полные графы. Двудольные графы. Подграфы;
6. 8.Минимальное остовное дерево. Алгоритм Прима. Алгоритм Краскала;
7. 9.Изоморфизм графов. Эйлеровы и гамильтоновы графы;
8. 11.Сравнимость чисел. Классы вычетов. Обратимые элементы по модулю m;
9. 12.Решение систем линейных уравнений в кольце вычетов по модулю;
10. 13.Функция Эйлера. Теорема Эйлера;
11. 14.Абелевы группы и их структура;
12. 15.Группы подстановок, лемма Бернсайда и теорема Пойа;
13. 16.Факторизация и дискретное логарифмирование;
14. 2.Спектральное представление булевых функций, нахождение их нелинейности, быстрое преобразование Уолша;
15. 10.Делимость чисел. Алгоритм Евклида. Факторизация числа;
16. 1.Способы представления булевых функций и их оптимизация.

3.4. Темы лабораторных работ

1. 7.Нахождение числа неизоморфных графов с заданными характеристиками;
2. 6.Линеаризация наибольшего общего делителя;
3. 1.Быстрое преобразование Мёбиуса для оптимизации булевой функции;
4. 2.Спектральное представление булевых функций и нахождение их нелинейности с помощью быстрого преобразования Уолша;
5. 3.Схемы распределения шаров по ящикам;
6. 8.Методы факторизации и дискретного логарифмирования;
7. 5.Классификация булевых функций;
8. 4.Решение рекуррентных соотношений.

3.5 Консультации

Групповые консультации по разделам дисциплины (ГК)

1. Обсуждение материалов по кейсам раздела "Булевы функции и их криптографические свойства"
2. Обсуждение материалов по кейсам раздела "Комбинаторные методы"
3. Обсуждение материалов по кейсам раздела "Графы и преобразования"
4. Обсуждение материалов по кейсам раздела "Алгебраические структуры и основы модулярной арифметики"

Текущий контроль (ТК)

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Булевы функции и их криптографические свойства"

2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Комбинаторные методы"
3. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Графы и преобразования"
4. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Алгебраические структуры и основы модулярной арифметики"

3.6 Тематика курсовых проектов/курсовых работ

Курсовой проект/ работа не предусмотрены

3.7. Соответствие разделов дисциплины и формируемых в них компетенций

Запланированные результаты обучения по дисциплине (в соответствии с разделом 1)	Коды индикаторов	Номер раздела дисциплины (в соответствии с п.3.1)				Оценочное средство (тип и наименование)
		1	2	3	4	
Знать:						
комбинаторные методы, теорию графов	ОПК-2(Компетенция)				+	Контрольная работа/Контрольная работа №4 «Алгебраические структуры и основы модулярной арифметики»
теорию булевых функций и алгебраических структур	ОПК-2(Компетенция)	+				Контрольная работа/Контрольная работа №1 «Булевы функции и их криптографические свойства»
Уметь:						
применять методы дискретной математики при решении прикладных задач	ОПК-2(Компетенция)			+		/Контрольная работа №3 «Графы»
анализировать свойства булевых функций и использовать булевы функции с требуемыми свойствами	ОПК-2(Компетенция)		+			Контрольная работа/Контрольная работа №2 «Комбинаторные методы»

4. КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ДИСЦИПЛИНЕ)

4.1. Текущий контроль успеваемости

5 семестр

Форма реализации: Письменная работа

1. Контрольная работа №1 «Булевы функции и их криптографические свойства» (Контрольная работа)
2. Контрольная работа №2 «Комбинаторные методы» (Контрольная работа)
3. Контрольная работа №3 «Графы» ()
4. Контрольная работа №4 «Алгебраические структуры и основы модулярной арифметики» (Контрольная работа)

Балльно-рейтинговая структура дисциплины является приложением А.

4.2 Промежуточная аттестация по дисциплине

Экзамен (Семестр №5)

Оценка определяется в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ» на основании семестровой и экзаменационной составляющих.

В диплом выставляется оценка за 5 семестр.

Примечание: Оценочные материалы по дисциплине приведены в фонде оценочных материалов ОПОП.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Печатные и электронные издания:

1. Гашков, С. Б. Дискретная математика : учебник и практикум для академического бакалавриата вузов по естественнонаучным направлениям / С. Б. Гашков, А. Б. Фролов . – 2-е изд., испр. и доп . – М. : Юрайт, 2018 . – 448 с. – (Бакалавр. Академический курс) . - ISBN 978-5-534-04435-5 .;
2. Гаврилов, Г. П. Задачи и упражнения по дискретной математике : учебное пособие / Г. П. Гаврилов, А. А. Сапоженко . – 3-е изд., перераб . – М. : Физматлит, 2006 . – 416 с. - ISBN 5-922104-77-2 .;
3. Набебин, А. А. Дискретная математика : учебник для вузов по специальностям "Прикладная математика и информатика", "Информационные системы и технологии" / А. А. Набебин . – М. : Научный мир, 2010 . – 512 с. - ISBN 978-5-91522-190-0 .;
4. Фомичев, В. М. Криптографические методы защиты информации: [в 2 ч.]. Ч. 1.: Математические аспекты : учебник для академического бакалавриата вузов по инженерно-техническим направлениям / В. М. Фомичев, Д. А. Мельников ; ред. В. М. Фомичев . – М. : Юрайт, 2018 . – 209 с. – (Бакалавр. Академический курс) . - ISBN 978-5-9916-7089-0 . - ISBN 978-5-9916-7088-3 .;
5. Таранников, Ю. В. Дискретная математика. Задачник : учебное пособие для академического бакалавриата, для вузов по естественнонаучным направлениям и специальностям / Ю. В. Таранников . – М. : Юрайт, 2016 . – 385 с. – (Бакалавр. Академический курс) . - ISBN 978-5-9916-6283-3 .;

6. Авдошин С. М., Набебин А. А.- "Дискретная математика. Модулярная алгебра, криптография, кодирование", Издательство: "ДМК Пресс", Москва, 2017 - (352 с.) https://e.lanbook.com/book/93575.

5.2 Лицензионное и свободно распространяемое программное обеспечение:
1. СДО "Прометей";
2. Office / Российский пакет офисных программ;
3. Windows / Операционная система семейства Linux;
4. Майнд Видеоконференции;
5. Acrobat Reader.

5.3 Интернет-ресурсы, включая профессиональные базы данных и информационно-справочные системы:
1. **ЭБС Лань** - https://e.lanbook.com/
2. **ЭБС "Университетская библиотека онлайн"** - http://biblioclub.ru/index.php?page=main_ub_red
3. **Научная электронная библиотека** - https://elibrary.ru/
4. **База данных ВИНИТИ online** - http://www.viniti.ru/
5. **База данных журналов издательства Elsevier** - https://www.sciencedirect.com/
6. **Электронные ресурсы издательства Springer** - https://link.springer.com/
7. **База данных Web of Science** - http://webofscience.com/
8. **База данных Scopus** - http://www.scopus.com
9. **Национальная электронная библиотека** - https://rusneb.ru/
10. **ЭБС "Консультант студента"** - http://www.studentlibrary.ru/

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Тип помещения	Номер аудитории, наименование	Оснащение
Учебные аудитории для проведения лекционных занятий и текущего контроля	Н-204, Учебная аудитория	парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, колонки звуковые, мультимедийный проектор, экран
	К-601, Учебная аудитория	парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, мультимедийный проектор, экран
Учебные аудитории для проведения практических занятий, КР и КП	М-510, Учебная аудитория	парта со скамьей, стол преподавателя, стул, доска меловая
Учебные аудитории для проведения промежуточной аттестации	М-510, Учебная аудитория	парта со скамьей, стол преподавателя, стул, доска меловая
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
Помещения для самостоятельной работы	НТБ-303, Компьютерный читальный зал	стол компьютерный, стул, стол письменный, вешалка для одежды, компьютерная сеть с выходом в Интернет, компьютер персональный, принтер, кондиционер
	К-307, Учебная лаборатория "Открытое программное	стол преподавателя, стол компьютерный, стол учебный, стул, вешалка для одежды, тумба,

	обеспечение"	компьютерная сеть с выходом в Интернет, мультимедийный проектор, экран, доска маркерная, сервер, компьютер персональный, кондиционер
	К-302, Учебная лаборатория "Информационно-аналитические технологии"	стол преподавателя, стол компьютерный, стул, мультимедийный проектор, экран, доска маркерная, сервер, компьютер персональный, кондиционер
Помещения для консультирования	М-510, Учебная аудитория	парта со скамьей, стол преподавателя, стул, доска меловая
Помещения для хранения оборудования и учебного инвентаря	К-202/2, Склад кафедры БИТ	стеллаж для хранения инвентаря, стол, стул, шкаф для документов, шкаф для хранения инвентаря, тумба, запасные комплектующие для оборудования

Приложение А

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Дискретная математика-2

(название дисциплины)

5 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

КМ-1 Контрольная работа №1 «Булевы функции и их криптографические свойства» (Контрольная работа)

КМ-2 Контрольная работа №2 «Комбинаторные методы» (Контрольная работа)

КМ-3 Контрольная работа №3 «Графы»

КМ-4 Контрольная работа №4 «Алгебраические структуры и основы модулярной арифметики» (Контрольная работа)

Вид промежуточной аттестации – Экзамен.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
		Неделя КМ:	4	8	12	15
1	Булевы функции и их криптографические свойства					
1.1	Булевы функции		+			
1.2	Криптографические свойства булевых функций		+			
2	Комбинаторные методы					
2.1	Общая комбинаторная схема			+		
2.2	Рекуррентные соотношения и производящие функции			+		
2.3	Классификация булевых функций			+		
3	Графы					
3.1	Элементы теории графов				+	
3.2	Графы преобразований и их свойства				+	
4	Алгебраические структуры и основы модулярной арифметики					
4.1	Алгебраические основы					+
4.2	Теоретико-числовые основы					+
		Вес КМ, %:	25	25	25	25