Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Национальный исследовательский университет «МЭИ»

Направление подготовки/специальность: 01.03.02 Прикладная математика и информатика

Наименование образовательной программы: Математическое моделирование

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

Рабочая программа дисциплины
МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Часть, формируемая участниками образовательных отношений**
№ дисциплины по учебному плану:	**Б4.Ч.02**
Трудоемкость в зачетных единицах:	**7 семестр - 2;**
Часов (всего) по учебному плану:	**72 часа**
Лекции	**7 семестр - 16 часов;**
Практические занятия	**7 семестр - 16 часов;**
Лабораторные работы	**не предусмотрено учебным планом**
Консультации	**проводится в рамках часов аудиторных занятий**
Самостоятельная работа	**7 семестр - 39,7 часа;**
в том числе на КП/КР	**не предусмотрено учебным планом**
Иная контактная работа	**проводится в рамках часов аудиторных занятий**
включая: **Тестирование** **Контрольная работа**	
Промежуточная аттестация:	
Зачет	**7 семестр - 0,3 часа;**

Москва 2018

ПРОГРАММУ СОСТАВИЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Фролов А.Б. Идентификатор: Ref8507cb-FrolovAB-a54b01e2	А.Б. Фролов
(должность)	(подпись)	(расшифровка подписи)

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Черепова М.Ф. Идентификатор: R9267877e-CherepovaMF-dbb9bf1	М.Ф. Черепова
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)
Заведующий выпускающей кафедры	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Зубков П.В. Идентификатор: R4920bc6f-ZubkovPV-8172426c	П.В. Зубков
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины: состоит в изучении основных задач и математических моделей и методов криптографии

Задачи дисциплины

- освоение криптографической терминологии, основных свойств криптографических преобразований;
- изучение формальных моделей шифров и открытых текстов, основных методов криптоанализа;
- приобретение навыков применения простейших шифров, построения их моделей, оценивания стойкости криптографического преобразования;
- формирование компетенций и результатов обучения по дисциплине в соответствии с индикаторами их достижения.

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**
ПК-2 Способен участвовать в компьютерной реализации математических моделей	ИД-5$_{ПК-2}$ Выбирает, модифицирует и реализует алгоритмы численной и алгебраической реализации математических моделей	знать: - криптографическую терминологию и основные задачи криптографии; - формальные модели шифров и кодов аутентификации. уметь: - применять простейшие шифры и строить формальные модели кодов аутентификации.
ПК-2 Способен участвовать в компьютерной реализации математических моделей	ИД-6$_{ПК-2}$ Демонстрирует понимание основ теории сложности реализации математических моделей	знать: - методы оценки качества криптографических преобразований.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к факультативным дисциплинам основной профессиональной образовательной программе Математическое моделирование (далее – ОПОП), направления подготовки 01.03.02 Прикладная математика и информатика, уровень образования: высшее образование - бакалавриат.

Требования к входным знаниям и умениям:

- знать общую алгебру, дискретную математику, теорию вероятностей и математическую статистику

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 2 зачетных единицы, 72 часа.

№ 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	Основные задачи и модели криптографии	18	7	4	-	4	-	-	-	-	-	10	-	***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Основные задачи и модели криптографии". ***Самостоятельное изучение теоретического материала:*** Повторение материала по разделу "Основные задачи и модели криптографии". ***Подготовка к текущему контролю:*** Подготовка к контрольной тесту № 1 "Криптографическая терминология и основные задачи криптографии" по разделу "Основные модели и задачи криптографии" ***Изучение материалов литературных источников:*** [1], стр. 37-54, 59-67 [2], стр. 7-8, 13-17 [4], стр. 157-160
1.1	Основные задачи и модели криптографии	18		4	-	4	-	-	-	-	-	10	-	
2	Комбинаторные блок-схемы в криптографии	18		4	-	4	-	-	-	-	-	10	-	***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу по разделу "Комбинаторные блок-схемы в криптографии". ***Самостоятельное изучение теоретического материала:*** Повторение материала по разделу "Комбинаторные блок-схемы в криптографии". ***Подготовка к текущему контролю:***
2.1	Комбинаторные блок-схемы в криптографии	18		4	-	4	-	-	-	-	-	10	-	

														Подготовка к тесту № 2 «Формальные модели шифров и кодов аутентификации». ***<u>Изучение материалов литературных источников:</u>*** [1], стр. 81-83 [2], стр. 17-20
3	Свойства криптографических преобразований	18		4	-	4	-	-	-	-	-	10	-	***<u>Самостоятельное изучение теоретического материала:</u>*** Изучение дополнительного материала по разделу "Свойства криптографических преобразований". ***<u>Самостоятельное изучение теоретического материала:</u>*** Повторение материала по разделу "Свойства криптографических преобразований". ***<u>Подготовка к контрольной работе:</u>*** Подготовка к контрольной работе «Применение простейших шифров и формальных моделей кодов аутентификации» по теме «Свойства криптографических преобразований» ***<u>Изучение материалов литературных источников:</u>*** [1], стр. 68-83 [2], стр. 17-20 [3], стр. 18-28
3.1	Свойства криптографических преобразований	18		4	-	4	-	-	-	-	-	10	-	
4	Надёжность шифров	17.7		4	-	4	-	-	-	-	-	9.7	-	***<u>Самостоятельное изучение теоретического материала:</u>*** Изучение дополнительного материала по разделу "Надежность шифров". ***<u>Самостоятельное изучение теоретического материала:</u>*** Повторение материала по разделу "Надежность шифров". ***<u>Подготовка к контрольной работе:</u>*** Подготовка к контрольной работе «Оценивание стойкости криптографического преобразования и надежности шифров»» по теме «Надежность шифров».
4.1	Надёжность шифров	17.7		4	-	4	-	-	-	-	-	9.7	-	
	Зачет	0.3		-	-	-	-	-	-	-	0.3	-	-	

	Всего за семестр	**72.0**		**16**	**-**	**16**	**-**	**-**	**-**	**-**	**0.3**	**39.7**	**-**	
	Итого за семестр	**72.0**		**16**	**-**	**16**	**-**		**-**		**0.3**	**39.7**		

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. Основные задачи и модели криптографии

1.1. Основные задачи и модели криптографии

Задачи криптографии: конфиденциальность, целостность, аутентификация. Формальные модели шифров: простой замены, перестановки, поточного шифра, блочного шифра. Модели открытых текстов: простейшая вероятностная модель, марковская модель, критерий на открытый ключ. Шифры гаммирования и методы их вскрытия.

2. Комбинаторные блок-схемы в криптографии

2.1. Комбинаторные блок-схемы в криптографии

Латинские квадраты, латинские прямоугольники, Ортогональные массивы. Имитостойкость шифров. Коды аутентификации и стратегии навязывания. Алгебраическая и вероятностная модели кода аутентификации. Вычисление вероятностей имитации и подмены сообщения. Нижние оценки вероятностей имитации и подмены сообщений.

3. Свойства криптографических преобразований

3.1. Свойства криптографических преобразований

Преобразования Фурье и Уолша-Адамара булевой функции. Матрицы Адамара и Сильвестра-Адамара. Преобразование Фурье булевой функции. Статистическая структура булевой функции и индуктивный метод ее построения. Преобразование Уолша – Адамара. Схема Грина быстрых преобразований Фурье и Уолша-Адамара. Метрическая трактовка элементов преобразования Уолша-Адамара. Статистические аналоги булевых функций. Бент функции. Расстояние до аффинных функций.

4. Надёжность шифров

4.1. Надёжность шифров

Энтропия случайной величины, энтропия и избыточность языка. Совместная и условная энтропия случайных величин. Теоретическая стойкость шифров. Совершенный шифр. Неопределенность шифра по ключу. Расстояние единственности. Практическая стойкость шифров.

3.3. Темы практических занятий

1. Модели открытых текстов: критерий на открытый ключ;
2. Теоретическая стойкость шифров. Совершенный шифр;
3. Статистические аналоги булевых функций. Бент функции. Расстояние до аффинных функций;
4. Схема Грина быстрых преобразований Фурье и Уолша-Адамара;
5. Статистическая структура булевой функции и индуктивный метод ее построения;
6. Вычисление вероятностей имитации и подмены сообщения;
7. Алгебраическая и вероятностная модели кода аутентификации;
8. Формальные модели шифров: шифры простой замены и перестановки.

3.4. Темы лабораторных работ

не предусмотрено

3.5 Консультации

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:						
формальные модели шифров и кодов аутентификации	ИД-5$_{ПК-2}$		+			Тестирование/Формальные модели шифров и кодов аутентификации
криптографическую терминологию и основные задачи криптографии	ИД-5$_{ПК-2}$	+				Тестирование/Криптографическая терминология и основные задачи криптографии
методы оценки качества криптографических преобразований	ИД-6$_{ПК-2}$				+	Контрольная работа/Оценивание стойкости криптографических преобразований и надежности шифров
Уметь:						
применять простейшие шифры и строить формальные модели кодов аутентификации	ИД-5$_{ПК-2}$			+		Контрольная работа/Применение простейших шифров и формальных моделей кодов аутентификации

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

4.1. Текущий контроль успеваемости

7 семестр

Форма реализации: Билеты (письменный опрос)

1. Формальные модели шифров и кодов аутентификации (Тестирование)

Форма реализации: Письменная работа

1. Оценивание стойкости криптографических преобразований и надежности шифров (Контрольная работа)
2. Применение простейших шифров и формальных моделей кодов аутентификации (Контрольная работа)

Форма реализации: Проверка задания

1. Криптографическая терминология и основные задачи криптографии (Тестирование)

Балльно-рейтинговая структура дисциплины является приложением А.

4.2 Промежуточная аттестация по дисциплине

Зачет (Семестр №7)

Оценка определяется по совокупности результатов текущего контроля успеваемости в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ»

В диплом выставляется оценка за 7 семестр.

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

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Печатные и электронные издания:

1. Лось, А. Б. Криптографические методы защиты информации : учебник для академического бакалавриата вузов по инженерно-техническим направлениям и специальностям / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков, Нац. исслед. ун-т "Высшая школа экономики" . – 2-е изд., испр . – М. : Юрайт, 2018 . – 473 с. – (Бакалавр. Академический курс) . - ISBN 978-5-534-01530-0 .;
2. Гашков, С. Б. Криптографические методы защиты информации : учебное пособие для вузов по направлению "Прикладная математика и информатика" и "Информационные технологии" / С. Б. Гашков, Э. А. Применко, М. А. Черепнев . – М. : АКАДЕМИЯ, 2010 . – 304 с. – (Высшее профессиональное образование) . - ISBN 978-5-7695-4962-5 .;
3. Алгебраический процессор : методическое пособие по курсам "Математические основы криптографии" и "Криптографические методы защиты информации" по всем направлениям подготовки АВТИ / А. Б. Фролов, А. Ю. Белова, М. В. Волокитин, [и др.], Моск. энерг. ин-т (МЭИ ТУ) . – М. : Издательский дом МЭИ, 2010 . – 48 с.;
4. 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. Python.

5.3 Интернет-ресурсы, включая профессиональные базы данных и информационно-справочные системы:
1. **ЭБС Лань** - https://e.lanbook.com/
2. **Электронная библиотека МЭИ (ЭБ МЭИ)** - http://elib.mpei.ru/login.php

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Тип помещения	Номер аудитории, наименование	Оснащение
Учебные аудитории для проведения лекционных занятий и текущего контроля	М-710, Учебная аудитория каф. МКМ	стол преподавателя, стол учебный, стул, доска меловая
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
Учебные аудитории для проведения практических занятий, КР и КП	М-808, Учебная аудитория	стол учебный, стул, доска меловая
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
Учебные аудитории для проведения промежуточной аттестации	М-710а, Учебная аудитория каф. МКМ	стол, 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
Помещения для консультирования	М-714, Преподавательская каф. МКМ	рабочее место сотрудника, стул, шкаф, шкаф для документов, шкаф для одежды, тумба, доска меловая, мультимедийный проектор, экран, книги, учебники, пособия
Помещения для хранения оборудования и учебного инвентаря	М-301/1, Кладовая	стул
	М-713/1, Учебно-научная лаборатория каф. МКМ	рабочее место сотрудника, стул, шкаф, шкаф для одежды, тумба, компьютерная сеть с выходом в Интернет, компьютер персональный, книги, учебники, пособия

Приложение А

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Математические методы криптографии

(название дисциплины)

7 семестр

Перечень контрольных мероприятий <u>текущего контроля</u> успеваемости по дисциплине:

КМ-1 Криптографическая терминология и основные задачи криптографии (Тестирование)
КМ-2 Формальные модели шифров и кодов аутентификации (Тестирование)
КМ-3 Применение простейших шифров и формальных моделей кодов аутентификации (Контрольная работа)
КМ-4 Оценивание стойкости криптографических преобразований и надежности шифров (Контрольная работа)

Вид промежуточной аттестации – Зачет.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
		Неделя КМ:	4	8	12	15
1	Основные задачи и модели криптографии					
1.1	Основные задачи и модели криптографии		+			
2	Комбинаторные блок-схемы в криптографии					
2.1	Комбинаторные блок-схемы в криптографии			+		
3	Свойства криптографических преобразований					
3.1	Свойства криптографических преобразований				+	
4	Надёжность шифров					
4.1	Надёжность шифров					+
Вес КМ, %:			25	25	25	25