Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Национальный исследовательский университет «МЭИ»

Направление подготовки/специальность: 01.04.02 Прикладная математика и информатика

Наименование образовательной программы: Математическое моделирование

Уровень образования: высшее образование - магистратура

Форма обучения: Очная

Рабочая программа дисциплины
МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ И РАСПОЗНАВАНИЯ ОБРАЗОВ

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Часть, формируемая участниками образовательных отношений**
№ дисциплины по учебному плану:	**Б1.Ч.04.03.01**
Трудоемкость в зачетных единицах:	**2 семестр - 5;** **3 семестр - 6;** **всего - 11**
Часов (всего) по учебному плану:	**396 часа**
Лекции	**2 семестр - 32 часа;** **3 семестр - 32 часа;** **всего - 64 часа**
Практические занятия	**2 семестр - 32 часа;** **3 семестр - 32 часа;** **всего - 64 часа**
Лабораторные работы	**не предусмотрено учебным планом**
Консультации	**2 семестр - 2 часа;** **3 семестр - 18 часов;** **всего - 20 часов**
Самостоятельная работа	**2 семестр - 113,5 часов;** **3 семестр - 129,2 часа;** **всего - 242,7 часа**
в том числе на КП/КР	**3 семестр - 15,7 часов;**
Иная контактная работа	**3 семестр - 4 часа;**
включая: **Расчетно-графическая работа** **Контрольная работа** **Проверочная работа**	
Промежуточная аттестация:	
Экзамен **Защита курсовой работы** **Экзамен**	**2 семестр - 0,5 часа;** **3 семестр - 0,3 часа;** **3 семестр - 0,5 часа;** **всего - 1,3 часа**

Москва 2020

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 математических методов распознавания образов и современных математических методов и протоколов защиты информации

Задачи дисциплины

- изучение основ теории распознавания образов;
- изучение основ теории и практики защиты информации;
- приобретение навыков применения математических методов распознавания образов к решению научных и практических задач и навыков применения криптографических примитивов в задачах обеспечения информационной безопасности.

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-1 Способен создавать, исследовать и реализовывать математические модели естествознания и технологий	ИД-3$_{ПК-1}$ Демонстрирует знание терминологии, основных понятий и методов решения прикладных задач	знать: - основные атаки на криптографические протоколы; - модели шифров симметричных криптосистем и криптосистемы с открытым ключом; - алгоритмы кластеризации, классификации и ранжирования; - методы распознавания частично-упорядоченных объектов и принцип конечной топологии; - принципы классификации и распознавания в метрических пространствах. уметь: - анализировать структуру блочного шифра.
ПК-1 Способен создавать, исследовать и реализовывать математические модели естествознания и технологий	ИД-5$_{ПК-1}$ Применяет современные методы исследования математических моделей	уметь: - применять готовые библиотеки программ для распознавания и анализировать работу поискового робота.
ПК-1 Способен создавать, исследовать и реализовывать математические модели естествознания и технологий	ИД-6$_{ПК-1}$ Разрабатывает и исследует алгоритмы численного решения прикладных задач	знать: - российские криптографические стандарты. уметь: - создавать исполнимые спецификации криптографических протоколов.
ПК-1 Способен создавать, исследовать и реализовывать математические модели естествознания и	ИД-7$_{ПК-1}$ Анализирует результаты численного и аналитического решения прикладных задач	уметь: - анализировать стойкость схем шифрования.

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения
технологий		

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к основной профессиональной образовательной программе Математическое моделирование (далее – ОПОП), направления подготовки 01.04.02 Прикладная математика и информатика, уровень образования: высшее образование - магистратура.

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 11 зачетных единиц, 396 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	Задачи защиты информации криптографическими методами и виды атак	12	2	2	-	2	-	-	-	-	-	8	-	***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "задачи защиты информации криптографическими методами и виды атак". ***Изучение материалов литературных источников:*** [1], стр. 42-46 [4], стр. 4-20
1.1	Задачи защиты информации криптографическими методами и виды атак	12		2	-	2	-	-	-	-	-	8	-	
2	Распределение ключей в компьютерной сети. Разделение секрета	24		6	-	6	-	-	-	-	-	12	-	***Подготовка к контрольной работе:*** Подготовка к контрольной работе №1 по теме «Распределение ключей в компьютерной сети». ***Изучение материалов литературных источников:*** [1], стр. 375-400 [2], стр. 100-106 [3], стр. 55-63
2.1	Распределение ключей в компьютерной сети. Разделение секрета	24		6	-	6	-	-	-	-	-	12	-	
3	Блочные системы шифрования	24		6	-	6	-	-	-	-	-	12	-	***Подготовка к контрольной работе:*** Подготовка к контрольной работе № 2 по темам «Блочные системы шифрования». ***Изучение материалов литературных источников:*** [1], стр. 209-269
3.1	Блочные системы шифрования	24		6	-	6	-	-	-	-	-	12	-	
4	Хеш-функции и их применение	12		2	-	2	-	-	-	-	-	8	-	***Подготовка к контрольной работе:*** Подготовка к контрольной работе №2 по теме «Блочные системы шифрования» . ***Изучение материалов литературных***
4.1	Хеш-функции и их применение	12		2	-	2	-	-	-	-	-	8	-	

														источников: [1], стр. 270-302
5	Криптосистемы с открытым ключом	18		4	-	4	-	-	-	-	-	10	-	***Подготовка к контрольной работе:*** Подготовка к контрольной работе №3 по теме «Криптосистемы с открытым ключом». ***Изучение материалов литературных источников:*** [1], стр. 321-359 [2], стр. 109-111 [3], стр. 63-54 [6], стр. 92-99
5.1	Криптосистемы с открытым ключом	18		4	-	4	-	-	-	-	-	10	-	
6	Протоколы с нулевым разглашением секрета	20		4	-	4	-	-	-	-	-	12	-	***Подготовка к контрольной работе:*** Подготовка к контрольной работе №3 по теме «Криптосистемы с открытым ключом» . ***Изучение материалов литературных источников:*** [3], стр. 75 [4], стр. 135-141
6.1	Протоколы с нулевым разглашением секрета	20		4	-	4	-	-	-	-	-	12	-	
7	Электронная цифровая подпись	20		4	-	4	-	-	-	-	-	12	-	***Подготовка к текущему контролю:*** Подготовка к контрольной работе №4 по теме «Электронная цифровая подпись». ***Изучение материалов литературных источников:*** [1], стр. 360-371 [2], стр. 112-121 [3], стр. 65-71 [4], стр. 144-158 [5], стр. 441-445
7.1	Электронная цифровая подпись	20		4	-	4	-	-	-	-	-	12	-	
8	Протоколы, основанные на спаривании	14		4	-	4	-	-	-	-	-	6	-	***Подготовка к текущему контролю:*** Подготовка к контрольной работе №4 по теме «Электронная цифровая подпись». ***Изучение материалов литературных источников:*** [2], стр. 139-145
8.1	Протоколы, основанные на спаривании	14		4	-	4	-	-	-	-	-	6	-	
	Экзамен	36.0		-	-	-	-	2	-	-	0.5	-	33.5	
	Всего за семестр	**180.0**		**32**	-	**32**	-	**2**	-	-	**0.5**	**80**	**33.5**	
	Итого за семестр	**180.0**		**32**	-	**32**	**2**		-		**0.5**	**113.5**		
9	Классификация и распознавание в	51	3	11	-	10	-	-	-	-	-	30	-	***Подготовка к контрольной работе:*** Изучение материалов по разделу

	метрических пространствах													Классификация и распознавание в метрических пространствах и подготовка к контрольной работе ***Изучение материалов литературных источников:*** [7], стр. 10-25
9.1	Классификация и распознавание в метрических пространствах	51		11	-	10	-	-	-	-	-	30	-	
10	Основные алгоритмы классификации и кластеризации и другие важные алгоритмы и задачи из области распознавания образов	67		13	-	14	-	-	-	-	-	40	-	***Подготовка к контрольной работе:*** Изучение материалов по разделу Основные алгоритмы классификации и кластеризации и другие важные алгоритмы и задачи из области распознавания образов и подготовка к контрольной работе ***Изучение материалов литературных источников:*** [8], стр. 26-33, 93-107, 137-156 [9], стр. 55-56, 351-354 [10], стр. 146-150, 223-227, 253-268 [11], стр. 37-44 [12], стр. 282-331
10.1	Основные алгоритмы классификации и кластеризации и другие важные алгоритмы и задачи из области распознавания образов	67		13	-	14	-	-	-	-	-	40	-	
11	Распознавание частично-упорядоченных объектов. Классификация и распознавание топологических форм	26		8	-	8	-	-	-	-	-	10	-	***Подготовка к контрольной работе:*** Изучение материалов по разделу Распознавание частично-упорядоченных объектов. Классификация и распознавание топологических форм и подготовка к контрольной работе ***Изучение материалов литературных источников:*** [7], стр. 74-105 [13], стр. 7-30
11.1	Распознавание частично-упорядоченных объектов. Классификация и распознавание топологических форм	26		8	-	8	-	-	-	-	-	10	-	
	Экзамен	36.0		-	-	-	-	2	-	-	0.5	-	33.5	
	Курсовая работа (КР)	36.0		-	-	-	16	-	4	-	0.3	15.7	-	
	Всего за семестр	**216.0**		**32**	**-**	**32**	**16**	**2**	**4**	**-**	**0.8**	**95.7**	**33.5**	

	Итого за семестр	**216.0**		**32**	**-**	**32**	**18**	**4**	**0.8**	**129.2**	
	ИТОГО	**396.0**	**-**	**64**	**-**	**64**	**20**	**4**	**1.3**	**242.7**	

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. Задачи защиты информации криптографическими методами и виды атак

1.1. Задачи защиты информации криптографическими методами и виды атак

Основные задачи криптографии: обеспечение конфиденциальности и целостности информации, аутентификация, предотвращение отказа от авторства. Процессы шифрования и расшифрования. Симметричные и асимметричные криптосистемы. Задача дешифрования. Виды криптографических атак. Примеры криптосистем.

2. Распределение ключей в компьютерной сети. Разделение секрета

2.1. Распределение ключей в компьютерной сети. Разделение секрета

Протоколы распределения ключей по открытым каналам: протокол Диффи-Хеллмана, протокол Месси-Омуры, MQV-протокол. Распределение ключей по секретным каналам. Схема Блома распределения ключей. Условия безопасности использования при компрометации части ключевого материала. KDP-схема предварительного распределения ключей. Протоколы распределения ключей с использованием симметричной криптосистемы. Протокол Ниидман-Шроедера. Протокол Kerberos. Сетевые протоколы. Протокол SSL и протоколы TLS. Атаки на SSl и TLS протоколы Уязвимости протоколов. Схемы разделения секрета. Проверяемое разделение секрета.

3. Блочные системы шифрования

3.1. Блочные системы шифрования

Принципы построения блочных систем шифрования. Схема Фейстеля. Блоки (этапы) нелинейного преобразования. Примеры блочных систем шифрования: стандарты шифрования DES, ГОСТ 28147-89, AES, Кузнечик. Криптоанализ блочных систем шифрования: метод компромисса «время-объем памяти», дифференциальный криптоанализ. Режимы использования блочных шифров. Код аутентификации сообщения.

4. Хеш-функции и их применение

4.1. Хеш-функции и их применение

Понятие криптографической хеш-функции. Бесключевые и ключевые хеш-функции и их свойства. Российский стандарт хеш-функции. Применение хэш-функций в финансовой криптографии. Электронные платежи. Системы Pay Word и MicroMint. Стандарты хеш-функций.

5. Криптосистемы с открытым ключом

5.1. Криптосистемы с открытым ключом

Криптосистема RSA, особенности выбора параметров, использование в компьютерной сети. Цифровая подпись RSA. Атака по выбираемому шифртексту. Криптосистема Рабина, ее теоретическая стойкость и условия однозначности расшифрования. Криптосистема Эль Гамаля, условия безопасности использования. Реализация в мультипликативной группе конечного поля и в группе точек эллиптической кривой. Криптосистемы Гольдвассер-Микали и Блума-Гольдвассер. Понятия семантически стойкой и полиномиально стойкой криптосистем. Полиномиально неразличимые вероятностные распределения. Битовая стойкость криптосистем использование частичной информации. Криптографическая стойкость генератора псевдослучайных чисел на основе проблемы квадратичного вычета. Инфраструктура открытого ключа.

6. Протоколы с нулевым разглашением секрета

6.1. Протоколы с нулевым разглашением секрета

Общая характеристика протоколов с нулевым разглашением секрета. Полнота и устойчивость. Протоколы при ограниченных вычислительных возможностях доказывающего: доказательство знания дискретного логарифма, протокол Фиата-Шамира, протокол Шнорра. Протоколы при неограниченных возможностях доказывающего: доказательство знания квадратичного вычета или квадратичного невычета. Протоколы с двусторонней ошибкой. Скрытая передача. Неинтерактивные протоколы с нулевым разглашением.

7. Электронная цифровая подпись

7.1. Электронная цифровая подпись

Понятие, назначение и необходимые свойства цифровой подписи. Цифровая подпись Эль Гамаля. Условия безопасного использования. Особенности Российского и американского стандартов цифровой подписи. Реализация в мультипликативной и аддитивной группах. Цифровая подпись с возвратом сообщения на эллиптических кривых. Цифровая подпись с личностным ключом проверки.

8. Протоколы, основанные на спаривании

8.1. Протоколы, основанные на спаривании

Билинейная проблема Диффи-Хеллмана. Вычислительный и распознающий варианты. Спаривание на эллиптических кривых. Свойства билинейности, и невырожденности. Протоколы, основанные на спаривании: однораундовый трехсторонний протокол Антуана Жу, Протокол короткой цифровой подписи, протокол шифрования личностным ключом.

9. Классификация и распознавание в метрических пространствах

9.1. Классификация и распознавание в метрических пространствах

Меры сходства объектов и их совокупностей. Некоторые алгоритмы кластеризации. Решающие функции и их свойства. Распознавание линейно разделимых образов. Персептрон, введение в нейронные сети. Метод потенциальных функций. Градиентные методы построения решающих функций. Построение решающей функции методом минимизации среднеквадратичной ошибки. Предварительная обработка образов. Отбор признаков и преобразование кластеров.

10. Основные алгоритмы классификации и кластеризации и другие важные алгоритмы и задачи из области распознавания образов

10.1. Основные алгоритмы классификации и кластеризации и другие важные алгоритмы и задачи из области распознавания образов

Библиотеки для работы с распознаванием образов. Анализ работы поискового робота. Латентное размещение Дирихле. Байесовский классификатор для текстов и изображений. Классификатор на базе деревьев решений. Нейронные сети. Метод опорных векторов. k-ближайшие соседи. Иерархическая кластеризация. Кластеризация методом k-средних. Многомерное шкалирование. Неотрицательная матричная факторизация. Оптимизация. Сверточные нейронные сети. Рекуррентные нейронные сети.

11. Распознавание частично-упорядоченных объектов. Классификация и распознавание топологических форм

11.1. Распознавание частично-упорядоченных объектов. Классификация и распознавание топологических форм

Функциональная интерпретация задачи распознавания. Алгоритмы разделения и распознавания. Общая схема. Алгоритмы разделения и распознавания. Примеры. Применение в молекулярной биологии. Сжатие генетического кода. Аналитические представления решающих правил. Понятие теста. Линейные тестовые алгоритмы распознавания. Алгоритм Кудрявцева голосования по тестам. Топологические формы. Некоторые модели топологических форм. Принцип конечной топологии. Классификация и распознавание. Распознавание оптических образов текстов.

3.3. Темы практических занятий

1. Примеры криптосистем. Виды криптографических атак;
2. Тестовый подход к распознаванию;
3. Распознавание частично-упорядоченных объектов;
4. Рекуррентные нейронные сети;
5. Сверточные нейронные сети;
6. Иерархическая кластеризация. Кластеризация методом k-средних. Многомерное шкалирование. Неотрицательная матричная факторизация. Оптимизация;
7. Классификатор на базе деревьев решений. Нейронные сети. Метод опорных векторов. k-ближайшие соседи;
8. Байесовский классификатор для текстов и изображений;
9. Анализ работы поискового робота;
10. Библиотеки для работы с распознаванием образов;
11. Предварительная обработка образов. Отбор признаков и преобразование кластеров;
12. Метод потенциальных функций. Градиентные методы построения решающих функций;
13. Решающие функции и их свойства. Распознавание линейно разделимых образов;
14. Некоторые алгоритмы кластеризации;
15. Меры сходства объектов и их совокупностей;
16. Протоколы, основанные на спаривании;
17. Цифровая подпись с личностным ключом проверки;
18. Цифровая подпись Эль Гамаля. Условия безопасного использования;
19. Протоколы с двусторонней ошибкой. Скрытая передача. Неинтерактивные протоколы с нулевым разглашением;
20. Протоколы доказательства с нулевым разглашением секрета при неограниченных возможностях доказывающего;
21. Протоколы аргументации с нулевым разглашением при ограниченных вычислительных возможностях доказывающего;
22. Криптосистемы с открытым ключом: Блюма-Гольдвассер;
23. Криптосистемы с открытым ключом: Эль Гамаля, Гольдвассер –Микали;
24. Криптосистемы с открытым ключом: RSA, Рабина;
25. Блочные криптосистемы;
26. Предварительное распределение ключей в компьютерной сети: KDP-схема;
27. Предварительное распределение ключей в компьютерной сети: схема Блома;
28. Протокол Керберос;
29. Протоколы распределения ключей по закрытым каналам;
30. Протоколы распределения ключей по открытым каналам;
31. Классификация и распознавание топологических форм;

32. Распознавание оптических образов текстов.

3.4. Темы лабораторных работ

не предусмотрено

3.5 Консультации

Аудиторные консультации по курсовому проекту/работе (КПР)

1. Консультации направлены на выполнение разделов курсового проекта под руководством наставника (преподавателя). В рамках часов на групповые консультации разбираются наиболее важные части расчетных заданий раздела "Классификация и распознавание в метрических пространствах"
2. Консультации направлены на выполнение разделов курсового проекта под руководством наставника (преподавателя). В рамках часов на групповые консультации разбираются наиболее важные части расчетных заданий раздела "Основные алгоритмы классификации и кластеризации и другие важные алгоритмы и задачи из области распознавания образов"
3. Консультации направлены на выполнение разделов курсового проекта под руководством наставника (преподавателя). В рамках часов на групповые консультации разбираются наиболее важные части расчетных заданий раздела "Распознавание частично-упорядоченных объектов. Классификация и распознавание топологических форм"

Групповые консультации по разделам дисциплины (ГК)

1. Обсуждение материалов раздела "Задачи защиты информации криптографическими методами и виды атак"
2. Обсуждение материалов раздела "Распределение ключей в компьютерной сети. Разделение секрета"
3. Обсуждение материалов раздела "Блочные системы шифрования"
4. Обсуждение материалов раздела "Хеш-функции и их применение"
5. Обсуждение материалов раздела "Криптосистемы с открытым ключом"
6. Обсуждение материалов раздела "Протоколы с нулевым разглашением секрета"
7. Обсуждение материалов раздела "Электронная цифровая подпись"
8. Обсуждение материалов раздела "Протоколы, основанные на спаривании"
9. Обсуждение материалов раздела "Классификация и распознавание в метрических пространствах"
10. Обсуждение материалов раздела "Основные алгоритмы классификации и кластеризации и другие важные алгоритмы и задачи из области распознавания образов"
11. Обсуждение материалов раздела "Распознавание частично-упорядоченных объектов. Классификация и распознавание топологических форм"

Индивидуальные консультации по курсовому проету /работе (ИККП)

1. Консультации проводятся по разделу "Классификация и распознавание в метрических пространствах"
2. Консультации проводятся по разделу "Основные алгоритмы классификации и кластеризации и другие важные алгоритмы и задачи из области распознавания образов"
3. Консультации проводятся по разделу "Распознавание частично-упорядоченных объектов. Классификация и распознавание топологических форм"

3.6 Тематика курсовых проектов/курсовых работ

3 Семестр

Курсовая работа (КР)

График выполнения курсового проекта

Неделя	1 - 4	5 - 8	9 - 12	13 - 15	Зачетная
Раздел курсового проекта	1	2	3	4	Защита курсового проекта
Объем раздела, %	25	25	25	25	-
Выполненный объем нарастающим итогом, %	25	50	75	100	-

Номер раздела	Раздел курсового проекта
1	Изучение материалов
2	Разработка плана программы
3	Составление программы
4	Отладка программы

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	5	6	7	8	9	10	11	
Знать:													
принципы классификации и распознавания в метрических пространствах	ИД-З$_{ПК-1}$									+			Контрольная работа/Принципы классификации и распознавания в метрических пространствах
методы распознавания частично-упорядоченных объектов и принцип конечной топологии	ИД-З$_{ПК-1}$											+	Контрольная работа/Методы распознавания частично-упорядоченных объектов и принцип конечной топологии
алгоритмы кластеризации, классификации и ранжирования	ИД-З$_{ПК-1}$										+		Контрольная работа/Алгоритмы кластеризации, классификации и ранжирования
модели шифров симметричных криптосистем и криптосистемы с открытым ключом	ИД-З$_{ПК-1}$					+	+						Контрольная работа/Криптосистемы с открытым ключом
основные атаки на криптографические протоколы	ИД-З$_{ПК-1}$			+	+								Контрольная работа/Блочные системы шифрования
российские криптографические стандарты	ИД-6$_{ПК-1}$							+	+				Проверочная работа/Электронная цифровая подпись
Уметь:													
анализировать структуру блочного шифра	ИД-З$_{ПК-1}$			+	+								Контрольная работа/Блочные системы шифрования
применять готовые библиотеки программ для распознавания и анализировать работу поискового робота	ИД-5$_{ПК-1}$										+		Контрольная работа/Библиотеки программ для распознавания и анализ работы поискового робота
создавать исполнимые спецификации криптографических протоколов	ИД-6$_{ПК-1}$	+	+										Расчетно-графическая работа/Распределение ключей в компьютерной сети

анализировать стойкость схем шифрования	ИД-7$_{ПК-1}$					+	+						Контрольная работа/Криптосистемы с открытым ключом

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

4.1. Текущий контроль успеваемости

2 семестр

Форма реализации: Билеты (письменный опрос)

1. Блочные системы шифрования (Контрольная работа)
2. Криптосистемы с открытым ключом (Контрольная работа)
3. Электронная цифровая подпись (Проверочная работа)

Форма реализации: Защита задания

1. Распределение ключей в компьютерной сети (Расчетно-графическая работа)

3 семестр

Форма реализации: Билеты (письменный опрос)

1. Алгоритмы кластеризации, классификации и ранжирования (Контрольная работа)
2. Библиотеки программ для распознавания и анализ работы поискового робота (Контрольная работа)
3. Методы распознавания частично-упорядоченных объектов и принцип конечной топологии (Контрольная работа)
4. Принципы классификации и распознавания в метрических пространствах (Контрольная работа)

Балльно-рейтинговая структура дисциплины является приложением А.
Балльно-рейтинговая структура курсовой работы является приложением Б.

4.2 Промежуточная аттестация по дисциплине

Экзамен (Семестр №2)

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

Экзамен (Семестр №3)

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

Курсовая работа (КР) (Семестр №3)

Оценка за курсовую работу определяется в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ»

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. Болотов, А. А. Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых / А. А. Болотов, С. Б. Гашков, А. Б. Фролов . – 3-е изд., испр. и доп . – М. : Эдиториал УРСС, 2019 . – 376 с. – (Основы защиты информации ; № 4) . - ISBN 978-5-9710-5813-7 .;
3. Болотов, А. А. Криптографические протоколы на эллиптических кривых : учебное пособие по курсу "Криптографические методы защиты информации" по всем направлениям / А. А. Болотов, С. Б. Гашков, А. Б. Фролов, Моск. энерг. ин-т (МЭИ ТУ) . – М. : Издательский дом МЭИ, 2007 . – 84 с. - ISBN 978-5-383-00093-9 .;
4. 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 .;
5. 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 .;
6. Фролов, А. Б. Псевдослучайные последовательности. Лабораторный практикум по криптографическим методам защиты информации : учебное пособие по курсам "Математические основы криптографии", "Криптографические методы защиты информации" по направлениям 230100 "Вычислительная техника и информатика", 010500 "Прикладная математика и информатика" / А. Б. Фролов, Нац. исслед. ун-т "МЭИ" . – М. : Издательский дом МЭИ, 2012 . – 100 с. - ISBN 978-5-383-00722-8 .
http://elib.mpei.ru/action.php?kt_path_info=ktcore.SecViewPlugin.actions.document&fDocumentId=4056;
7. Болотов, А. А. Классификация и распознавание в дискретных системах:Учебное пособие по курсу"Математическое моделирование дискретных систем" / А. А. Болотов, А. Б. Фролов, Моск. энерг. ин-т (МЭИ ТУ) . – М. : Изд-во МЭИ, 1997 . – 120 с. - ISBN 5-7046-0261-4 : 7.00 .;
8. Коэльо Л. П., Ричарт В.- "Построение систем машинного обучения на языке Python", (2-е изд.), Издательство: "ДМК Пресс", Москва, 2016 - (302 с.)
http://e.lanbook.com/books/element.php?pl1_id=82818;
9. Рашка С.- "Python и машинное обучение: крайне необходимое пособие по новейшей предсказательной аналитике, обязательное для более глубокого понимания методологии машинного обучения", Издательство: "ДМК Пресс", Москва, 2017 - (418 с.)
https://e.lanbook.com/book/100905;
10. Флах П.- "Машинное обучение. Наука и искусство построения алгоритмов, которые извлекают знания из данных", Издательство: "ДМК Пресс", Москва, 2015 - (400 с.)
http://e.lanbook.com/books/element.php?pl1_id=69955;
11. Шарден Б., Массарон Л., Боскетти А.- "Крупномасштабное машинное обучение вместе с Python", Издательство: "ДМК Пресс", Москва, 2018 - (358 с.)
https://e.lanbook.com/book/105836;
12. Гудфеллоу Я., Бенджио И., Курвилль А.- "Глубокое обучение", (2-е изд.), Издательство: "ДМК Пресс", Москва, 2018 - (652 с.)
https://e.lanbook.com/book/107901;
13. Фролов, А. Б. Классификация и распознавание топологических форм : учебное пособие по курсам "Современные проблемы прикладной математики и информатики" и "Современные компьютерные технологии в науке и образовании" по специальностям "Прикладная математика" и "Информационные системы и технологии" / А. Б. Фролов, Моск. энерг. ин-т (МЭИ ТУ) ; Ред. В. Б. Кудрявцев . – М. : Издательский дом МЭИ, 2010 . – 52 с. - ISBN 978-5-383-00460-9 .

http://elib.mpei.ru/action.php?kt_path_info=ktcore.SecViewPlugin.actions.document&fDocumentId=2133.

5.2 Лицензионное и свободно распространяемое программное обеспечение:
1. СДО "Прометей";
2. Office;
3. Windows;
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-710а, Учебная аудитория каф. МКМ	стол, стул, доска меловая
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
Учебные аудитории для проведения практических занятий, КР и КП	М-710а, Учебная аудитория каф. МКМ	стол, 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

Методы защиты информации и распознавания образов

(название дисциплины)

2 семестр

Перечень контрольных мероприятий <u>текущего контроля</u> успеваемости по дисциплине:
КМ-1 Распределение ключей в компьютерной сети (Расчетно-графическая работа)
КМ-2 Блочные системы шифрования (Контрольная работа)
КМ-3 Криптосистемы с открытым ключом (Контрольная работа)
КМ-4 Электронная цифровая подпись (Проверочная 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	Задачи защиты информации криптографическими методами и виды атак					
1.1	Задачи защиты информации криптографическими методами и виды атак		+			
2	Распределение ключей в компьютерной сети. Разделение секрета					
2.1	Распределение ключей в компьютерной сети. Разделение секрета		+			
3	Блочные системы шифрования					
3.1	Блочные системы шифрования			+		
4	Хеш-функции и их применение					
4.1	Хеш-функции и их применение			+		
5	Криптосистемы с открытым ключом					
5.1	Криптосистемы с открытым ключом				+	
6	Протоколы с нулевым разглашением секрета					
6.1	Протоколы с нулевым разглашением секрета				+	
7	Электронная цифровая подпись					
7.1	Электронная цифровая подпись					+
8	Протоколы, основанные на спаривании					

8.1	Протоколы, основанные на спаривании				+
	Вес КМ, %:	25	25	25	25

3 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

КМ-5 Принципы классификации и распознавания в метрических пространствах (Контрольная работа)

КМ-6 Библиотеки программ для распознавания и анализ работы поискового робота (Контрольная работа)

КМ-7 Алгоритмы кластеризации, классификации и ранжирования (Контрольная работа)

КМ-8 Методы распознавания частично-упорядоченных объектов и принцип конечной топологии (Контрольная работа)

Вид промежуточной аттестации – Экзамен.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-5	КМ-6	КМ-7	КМ-8
		Неделя КМ:	4	8	12	15
1	Классификация и распознавание в метрических пространствах					
1.1	Классификация и распознавание в метрических пространствах		+			
2	Основные алгоритмы классификации и кластеризации и другие важные алгоритмы и задачи из области распознавания образов					
2.1	Основные алгоритмы классификации и кластеризации и другие важные алгоритмы и задачи из области распознавания образов			+	+	
3	Распознавание частично-упорядоченных объектов. Классификация и распознавание топологических форм					
3.1	Распознавание частично-упорядоченных объектов. Классификация и распознавание топологических форм					+
	Вес КМ, %:		25	25	25	25

Приложение Б

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА КУРСОВОГО ПРОЕКТА/РАБОТЫ ПО ДИСЦИПЛИНЕ

Методы защиты информации и распознавания образов

(название дисциплины)

3 семестр

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

КМ-1 Оценка выполнение раздела № 1 «Изучение материалов»
КМ-2 Оценка выполнение раздела № 2 «Разработка плана программы»
КМ-3 Оценка выполнение раздела № 3 «Составление программы»
КМ-4 Оценка выполнение раздела № 4. «Отладка программы»

Вид промежуточной аттестации – защита КР.

Номер раздела	Раздел курсового проекта/курсовой работы	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
		Неделя КМ:	4	8	12	15
1	Изучение материалов		+			
2	Разработка плана программы			+		
3	Составление программы				+	
4	Отладка программы					+
		Вес КМ, %:	25	25	25	25