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 и компьютерное моделирование

Уровень образования: высшее образование - магистратура

Форма обучения: Очная

Рабочая программа дисциплины
КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Часть, формируемая участниками образовательных отношений**
№ дисциплины по учебному плану:	**Б1.Ч.06.02.01**
Трудоемкость в зачетных единицах:	**2 семестр - 5;**
Часов (всего) по учебному плану:	**180 часов**
Лекции	**2 семестр - 32 часа;**
Практические занятия	**2 семестр - 32 часа;**
Лабораторные работы	**не предусмотрено учебным планом**
Консультации	**2 семестр - 2 часа;**
Самостоятельная работа	**2 семестр - 113,5 часов;**
в том числе на КП/КР	**не предусмотрено учебным планом**
Иная контактная работа	**проводится в рамках часов аудиторных занятий**
включая: **Решение задач** **Тестирование**	
Промежуточная аттестация:	
Экзамен	**2 семестр - 0,5 часа;**

Москва 2023

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 современных математических методов преобразования информации для обеспечения ее конфиденциальности, целостности, аутентичности, а также скрытия ее передачи

Задачи дисциплины

- изучение основных понятий и задач криптографии;
- освоение криптографических преобразований и методов их применения в современных криптографических схемах;
- приобретение навыков применения современных криптографических протоколов для 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 разрабатывать и исследовать математические модели естествознания и технологий, а также осуществлять их компьютерную реализацию	ИД-З$_{ПК-1}$ Демонстрирует знание терминологии, основных понятий и методов решения и компьютерного моделирования прикладных задач	знать: - основные задачи криптографии, формальные модели шифров; основные свойства криптографических преобразований; перемешивающие свойства отображений. уметь: - строить формальные модели шифров, преобразования Фурье и Уолша-Адамара булевых функций, статистическую структуру булевой функции, вычислять расстояние между булевыми функциями.
ПК-1 Способен разрабатывать и исследовать математические модели естествознания и технологий, а также осуществлять их компьютерную реализацию	ИД-6$_{ПК-1}$ Разрабатывает и исследует алгоритмы компьютерного моделирования прикладных задач	знать: - формальное определение, структуру и режимы использования блочного шифра и методы построения функций хеширования; отечественные и зарубежные стандарты блочных шифров и функций хеширования. уметь: - строить структурные элементы блочного шифра и криптографических функций хеширования.
ПК-1 Способен разрабатывать и исследовать математические модели естествознания и технологий, а также осуществлять их компьютерную реализацию	ИД-7$_{ПК-1}$ Проводит компьютерное моделирование прикладных задач и анализирует его результаты	знать: - основные методы асимметричного шифрования; гибридную схему шифрования; схемы электронной подписи типа Эль-Гамаля и Шнорра; отечественные и зарубежные стандарты электронной подписи; - протоколы аргументации и доказательства с нулевым

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения
		разглашением; способы распределения ключевой информации в компьютерной сети. уметь: - моделировать схемы шифрования RSA, Рабина и Эль-Гамаля, электронной подписи типа Эль-Гамаля и Шнорра и анализировать их стойкость; - моделировать протоколы аргументации с нулевым разглашением, протоколы доказательства с нулевым разглашением и протоколы распределения ключевой информации в компьютерной сети.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к основной профессиональной образовательной программе Математическое и компьютерное 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 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	Криптография и ее задачи. Формальные модели шифров	12	2	2	-	2	-	-	-	-	-	8	-	***Подготовка к текущему контролю:*** Подготовка к Тесту № 1 «Формальные модели шифров».
1.1	Криптография и ее задачи. Формальные модели шифров	12		2	-	2	-	-	-	-	-	8	-	***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Криптография и ее задачи. Формальные модели шифров" ***Подготовка к текущему контролю:*** Повторение материала по разделу "Криптография и ее задачи. Формальные модели шифров" ***Изучение материалов литературных источников:*** [1], стр. 42-56 [4], стр. 4-20 [7], стр. 157-160
2	Свойства криптографических преобразований и их компьютерный анализ	24		6	-	6	-	-	-	-	-	12	-	***Подготовка к текущему контролю:*** Подготовка к Контрольной работе №1 «Криптографические преобразования».
2.1	Свойства криптографических преобразований и их компьютерный анализ	24		6	-	6	-	-	-	-	-	12	-	***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Свойства криптографических преобразований и их компьютерный анализ" ***Подготовка к текущему контролю:*** Повторение материала по разделу "Свойства криптографических преобразований и их

														компьютерный анализ" ***Изучение материалов литературных источников:*** [1], стр. 97-126
3	Блочные системы шифрования	24		6	-	6	-	-	-	-	-	12	-	***Подготовка к текущему контролю:*** Подготовка к Тесту № 2 «Блочные шифры и функции хеширования». ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Блочные системы шифрования" ***Подготовка к текущему контролю:*** Повторение материала по разделу "Блочные системы шифрования" ***Изучение материалов литературных источников:*** [1], стр. 209-269
3.1	Блочные системы шифрования	24		6	-	6	-	-	-	-	-	12	-	
4	Функции и алгоритмы хеширования	12		2	-	2	-	-	-	-	-	8	-	***Подготовка к текущему контролю:*** Подготовка к Контрольной работе №2 «Структурные элементы блочного шифра и функций хеширования». ***Подготовка к текущему контролю:*** Повторение материала по разделу "Функции и алгоритмы хеширования" ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Хеш-функции и их применение" ***Изучение материалов литературных источников:*** [1], стр. 270-279, 283-289
4.1	Хеш-функции и их применение	12		2	-	2	-	-	-	-	-	8	-	
5	Асимметричные криптосистемы	18		4	-	4	-	-	-	-	-	10	-	***Подготовка к текущему контролю:*** Подготовка к Тесту № 3 «Асимметричное шифрование и электронная подпись». ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Асимметричные криптосистемы" ***Подготовка к текущему контролю:***
5.1	Асимметричные криптосистемы	18		4	-	4	-	-	-	-	-	10	-	

														Повторение материала по разделу "Асимметричные криптосистемы" ***Изучение материалов литературных источников:*** [1], стр. 321-359 [2], стр. 109-112 [3], стр. 63-64 [6], стр. 92-99
6	Электронная цифровая подпись	20		4	-	4	-	-	-	-	-	12	-	***Подготовка к текущему контролю:*** Подготовка к Контрольной работе № 3 «Анализ и моделирование асимметричных криптосистем и электронной подписи». ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Электронная цифровая подпись" ***Подготовка к текущему контролю:*** Повторение материала по разделу "Электронная цифровая подпись" ***Изучение материалов литературных источников:*** [1], стр. 360-371 [2], стр. 112-119 [3], стр. 75 [4], стр. 135-141 [5], стр. 467-470
6.1	Электронная цифровая подпись	20		4	-	4	-	-	-	-	-	12	-	
7	Аутентификация с нулевым разглашением секрета. Скрытая передача	20		4	-	4	-	-	-	-	-	12	-	***Подготовка к текущему контролю:*** Подготовка к Тесту № 4 «Протоколы с нулевым разглашением». ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Аутентификация с нулевым разглашением секрета. Скрытая передача" ***Подготовка к текущему контролю:*** Повторение материала по разделу "Аутентификация с нулевым разглашением секрета. Скрытая передача" ***Изучение материалов литературных***
7.1	Аутентификация с нулевым разглашением секрета. Скрытая передача	20		4	-	4	-	-	-	-	-	12	-	

														источников: [2], стр. 122-138 [3], стр. 71-75 [4], стр. 144-158
8	Управление ключами. Ключевые системы беспроводных сенсорных сетей	14		4	-	4	-	-	-	-	-	6	-	***Подготовка к текущему контролю:*** Подготовка к Контрольной работе № 4 «Моделирование протоколов с нулевым разглашением и протоколов распределения ключей». ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Управление ключами. Ключевые системы беспроводных сенсорных сетей" ***Подготовка к текущему контролю:*** Повторение материала по разделу "Управление ключами. Ключевые системы беспроводных сенсорных сетей" ***Изучение материалов литературных источников:*** [1], стр. 375-399 [2], стр. 100-109 [5], стр. 170-178
8.1	Управление ключами. Ключевые системы беспроводных сенсорных сетей	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**		

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. Криптография и ее задачи. Формальные модели шифров

1.1. Криптография и ее задачи. Формальные модели шифров

Криптография как наука о математических методах преобразования информации для обеспечения ее конфиденциальности и целостности, аутентичности, предотвращения отказа от авторства, а также скрытия факта передачи информации. Алгебраическая и вероятностная модели шифра. Шифры простой замены и перестановки..

2. Свойства криптографических преобразований и их компьютерный анализ

2.1. Свойства криптографических преобразований и их компьютерный анализ

Разложения булевых функций, статистическая структура и статистические аналоги булевых функций, расстояние между булевыми функциями. Бент-функции. Корреляционно-иммунные функции. Строгий лавинный критерий. Критерий распространения. Группа инерции. Сильная равновероятость булевых функций. Семейство координатных булевых функций. Перемешивающие свойства отображений.

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, «Магма» ГОСТ 28147-89, AES, «Кузнечик» ГОСТ Р34.12-2015. Криптоанализ блочных систем шифрования: метод компромисса «время-объем памяти», дифференциальный криптоанализ. Режимы использования блочных шифров. Код аутентификации сообщения.

4. Функции и алгоритмы хеширования

4.1. Хеш-функции и их применение

Понятие криптографической хеш-функции. Бесключевые и ключевые хеш-функции и их свойства. Российский стандарт хеш-функции ГОСТ Р 34.11-94. Функция «Стрибог» ГОСТ Р 34.11-2-2012. Применение хэш-функций в финансовой криптографии. Электронные платежи. Системы Pay Word и MicroMint.

5. Асимметричные криптосистемы

5.1. Асимметричные криптосистемы

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. Гибридные криптосистемы.

6. Электронная цифровая подпись

6.1. Электронная цифровая подпись

Понятие, назначение и необходимые свойства цифровой подписи. Цифровая подпись Эль Гамаля. Условия безопасного использования. Реализация в мультипликативной и аддитивной группах. Особенности Российского ГОСТ Р 34.11-2-2012 и американского ECDSA

стандартов цифровой подписи. Цифровая подпись с возвратом сообщения на эллиптических кривых. Цифровая подпись с личностным ключом проверки.

7. Аутентификация с нулевым разглашением секрета. Скрытая передача

7.1. Аутентификация с нулевым разглашением секрета. Скрытая передача

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.

8. Управление ключами. Ключевые системы беспроводных сенсорных сетей

8.1. Управление ключами. Ключевые системы беспроводных сенсорных сетей

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 Нидмэн-Шроедера. Протокол Kerberos. Сетевые протоколы. Протокол SSL и протоколы TLS. Атаки на SSl и TLS протоколы. Ключевые системы беспроводных сенсорных сетей.

3.3. Темы практических занятий

1. Криптоанализ блочных систем шифрования: метод компромисса «время-объем памяти», дифференциальный криптоанализ. Режимы использования блочных шифров. Код аутентификации сообщения;
2. Протоколы с двусторонней ошибкой. Скрытая передача. Неинтерактивные протоколы с нулевым разглашением;
3. Протоколы аутентификации с нулевым разглашением;
4. Цифровая подпись с возвратом сообщения на эллиптических кривых. Цифровая подпись с личностным ключом проверки.;
5. Цифровая подпись Эль Гамаля. Стандарты цифровой подписи;
6. Гомоморфные криптосистемы с открытым ключом;
7. Криптосистемы с открытым ключом: RSA, Рабина, Эль Гамаля, Гольдвассер – Микали, Блюма-Гольдвассер;
8. Алгебраическая и вероятностная модели шифра. Шифры простой замены и перестановки;
9. Бесключевые и ключевые хеш-функции и их свойства. Применение хеш-функции;
10. Принципы построения блочных систем шифрования. Схема Фейстеля. Блоки (этапы) нелинейного преобразования;
11. Сильная равновероятость булевых функций. Семейство координатных булевых функций. Перемешивающие свойства отображений;
12. Строгий лавинный критерий. Критерий распространения;
13. Разложения Фурье и Уолша – Адамара. Статистическая структура булевой функции;
14. Цифровая подпись Эль Гамаля. Условия безопасного использования;
15. Протоколы распределения ключей по закрытым каналам;

16. Примеры блочных систем шифрования: стандарты шифрования;
17. Протоколы распределения ключей по открытым каналам.

3.4. Темы лабораторных работ

не предусмотрено

3.5 Консультации

Групповые консультации по разделам дисциплины (ГК)

1. Обсуждение материалов по кейсам раздела "Криптография и ее задачи. Формальные модели шифров"
2. Обсуждение материалов по кейсам раздела "Свойства криптографических преобразований и их компьютерный анализ"
3. Обсуждение материалов по кейсам раздела "Блочные системы шифрования"
4. Обсуждение материалов по кейсам раздела "Хеш-функции и их применение"
5. Обсуждение материалов по кейсам раздела "Асимметричные криптосистемы"
6. Обсуждение материалов по кейсам раздела "Электронная цифровая подпись"
7. Обсуждение материалов по кейсам раздела "Аутентификация с нулевым разглашением секрета. Скрытая передача"
8. Обсуждение материалов по кейсам раздела "Управление ключами. Ключевые системы беспроводных сенсорных сетей"

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	5	6	7	8	
Знать:										
основные задачи криптографии, формальные модели шифров; основные свойства криптографических преобразований; перемешивающие свойства отображений	ИД-3$_{ПК-1}$	+	+							Решение задач/Формальные модели шифров. Свойства криптографических преобразований
формальное определение, структуру и режимы использования блочного шифра и методы построения функций хеширования; отечественные и зарубежные стандарты блочных шифров и функций хеширования	ИД-6$_{ПК-1}$			+	+					Тестирование/Блочные шифры и функции хеширования
протоколы аргументации и доказательства с нулевым разглашением; способы распределения ключевой информации в компьютерной сети	ИД-7$_{ПК-1}$							+	+	Тестирование/Протоколы с нулевым разглашением. Аутентификация с нулевым разглашением секрета. Скрытая передача
основные методы асимметричного шифрования; гибридную схему шифрования; схемы электронной подписи типа Эль-Гамаля и Шнорра; отечественные и зарубежные стандарты электронной подписи	ИД-7$_{ПК-1}$					+	+			Тестирование/Асимметричное шифрование и электронная подпись
Уметь:										
строить формальные модели шифров, преобразования Фурье и Уолша-Адамара булевых функций, статистическую структуру булевой функции, вычислять расстояние между булевыми функциями	ИД-3$_{ПК-1}$	+	+							Решение задач/Формальные модели шифров. Свойства криптографических преобразований
строить структурные элементы блочного шифра и криптографических функций хеширования	ИД-6$_{ПК-1}$			+	+					Тестирование/Блочные шифры и функции хеширования

моделировать протоколы аргументации с нулевым разглашением, протоколы доказательства с нулевым разглашением и протоколы распределения ключевой информации в компьютерной сети	ИД-7$_{ПК-1}$							+	+	Тестирование/Протоколы с нулевым разглашением. Аутентификация с нулевым разглашением секрета. Скрытая передача
моделировать схемы шифрования RSA, Рабина и Эль-Гамаля, электронной подписи типа Эль-Гамаля и Шнорра и анализировать их стойкость	ИД-7$_{ПК-1}$					+	+			Тестирование/Асимметричное шифрование и электронная подпись

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. Асимметричное шифрование и электронная подпись (Тестирование)
2. Блочные шифры и функции хеширования (Тестирование)
3. Протоколы с нулевым разглашением. Аутентификация с нулевым разглашением секрета. Скрытая передача (Тестирование)

Форма реализации: Письменная работа

1. Формальные модели шифров. Свойства криптографических преобразований (Решение задач)

Балльно-рейтинговая структура дисциплины является приложением А.

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.

В диплом выставляется оценка за 2 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. 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 студентов вузов, обучающихся по естественнонаучным направлениям / С. Б. Гашков, А. Б. Фролов . – 3-е изд.,

испр. и доп . – Москва : Юрайт, 2020 . – 483 с. – (Высшее образование) . - ISBN 978-5-534-11613-7 .;
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. 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-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-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

Криптографические методы защиты информации

(название дисциплины)

2 семестр

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

КМ-1 Формальные модели шифров. Свойства криптографических преобразований (Решение задач)

КМ-2 Блочные шифры и функции хеширования (Тестирование)

КМ-3 Асимметричное шифрование и электронная подпись (Тестирование)

КМ-4 Протоколы с нулевым разглашением. Аутентификация с нулевым разглашением секрета. Скрытая передача (Тестирование)

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	Криптография и ее задачи. Формальные модели шифров					
1.1	Криптография и ее задачи. Формальные модели шифров		+			
2	Свойства криптографических преобразований и их компьютерный анализ					
2.1	Свойства криптографических преобразований и их компьютерный анализ		+			
3	Блочные системы шифрования					
3.1	Блочные системы шифрования			+		
4	Функции и алгоритмы хеширования					
4.1	Хеш-функции и их применение			+		
5	Асимметричные криптосистемы					
5.1	Асимметричные криптосистемы				+	
6	Электронная цифровая подпись					
6.1	Электронная цифровая подпись				+	
7	Аутентификация с нулевым разглашением секрета. Скрытая передача					
7.1	Аутентификация с нулевым разглашением секрета. Скрытая передача					+

8	Управление ключами. Ключевые системы беспроводных сенсорных сетей				
8.1	Управление ключами. Ключевые системы беспроводных сенсорных сетей				+
	Вес КМ, %:	25	25	25	25