

**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 и программное обеспечение вычислительных машин и компьютерных сетей

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

**Рабочая программа дисциплины**  
**КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ**

<b>Блок:</b>	<b>Блок 1 «Дисциплины (модули)»</b>
<b>Часть образовательной программы:</b>	<b>Часть, формируемая участниками образовательных отношений</b>
<b>№ дисциплины по учебному плану:</b>	<b>Б1.Ч.11</b>
<b>Трудоемкость в зачетных единицах:</b>	<b>8 семестр - 3;</b>
<b>Часов (всего) по учебному плану:</b>	<b>108 часов</b>
<b>Лекции</b>	<b>8 семестр - 28 часа;</b>
<b>Практические занятия</b>	<b>8 семестр - 14 часов;</b>
<b>Лабораторные работы</b>	<b>8 семестр - 14 часов;</b>
<b>Консультации</b>	<b>8 семестр - 2 часа;</b>
<b>Самостоятельная работа</b>	<b>8 семестр - 49,5 часа;</b>
<b>в том числе на КП/КР</b>	<b>не предусмотрено учебным планом</b>
<b>Иная контактная работа</b>	<b>проводится в рамках часов аудиторных занятий</b>
<b>включая:</b> <b>Тестирование</b> <b>Лабораторная работа</b>	
<b>Промежуточная аттестация:</b>	
<b>Экзамен</b>	<b>8 семестр - 0,5 часа;</b>

**Москва 2026**

## ПРОГРАММУ СОСТАВИЛ:

Преподаватель

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Хорев П.Б.
	Идентификатор	Rdf0a0f96-KhorevPB-ab4b01e2

П.Б. Хорев

## СОГЛАСОВАНО:

Руководитель  
образовательной  
программы

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Ионова Т.В.
	Идентификатор	R5ac51726-IonovaTV-b9dd3591

Т.В. Ионова

Заведующий выпускающей  
кафедрой

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Варшавский П.Р.
	Идентификатор	R9a563c96-VarshavskyPR-efb4bbd

П.Р.  
Варшавский

## 1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

**Цель освоения дисциплины:** Приобретение необходимых теоретических знаний и практических навыков по применению криптографических методов защиты информации.

### Задачи дисциплины

- Ознакомление с принципами применения криптографических алгоритмов и протоколов при обеспечении информационной безопасности компьютерных систем и сетей;
- Представление способов анализа криптографических алгоритмов и протоколов;
- Обучение использованию криптографических средств защиты информации при разработке и эксплуатации программных систем;
- Получение навыков использования криптографических методов и средств для решения различных задач.

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-3 Способен выполнять анализ и работы по защите информации	ИД-1 <sub>ПК-3</sub> Формирует методы защиты информации и умеет применять их на практике	знать: - Способы управления криптографическими ключами и сертификатами открытых ключей;; - Современные технологии создания программных средств криптографической защиты информации; - Способы построения симметричных и асимметричных криптографических систем; - Особенности использования криптографических методов защиты информации при решении различных прикладных задач.  уметь: - Использовать методы и средства криптографической защиты информации при обеспечении информационной безопасности компьютерных систем и сетей; - Предлагать методы и средства повышения информационной безопасности компьютерных систем и сетей, основанные на криптографической защите информации; - Использовать методы и средства криптографической защиты информации для создания защищенного электронного документооборота.
ПК-3 Способен выполнять анализ и работы по	ИД-2 <sub>ПК-3</sub> Представляет результаты анализа	знать: - Тенденции развития криптографических методов защиты

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения
защите информации	состояния защиты данных и предлагает методы по ее улучшению	<p>информации;</p> <ul style="list-style-type: none"> <li>- Российские и международные стандарты в области криптографических алгоритмов и протоколов;</li> <li>- Достоинства и недостатки современных криптографических систем.</li> </ul> <p>уметь:</p> <ul style="list-style-type: none"> <li>- Разрабатывать новые безопасные информационные технологии с использованием криптографических методов и средств;</li> <li>- Использовать литературу и источники сети Интернет для получения информации о создании новых криптографических методов и средств защиты информации;</li> <li>- Определять цели и задачи разработки новых методов и программных средств криптографической защиты информации в компьютерных системах и сетях;</li> <li>- Анализировать эффективность используемых криптографических методов и средств защиты информации.</li> </ul>

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к основной профессиональной образовательной программе Математическое и программное обеспечение вычислительных машин и компьютерных сетей (далее – ОПОП), направления подготовки 01.03.02 Прикладная математика и информатика, уровень образования: высшее образование - бакалавриат.

Требования к входным знаниям и умениям:

- знать Методы и средства защиты данных в компьютерных системах и сетях
- уметь Программировать на языке высокого уровня с использованием инструментальных средств разработки

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 3 зачетных единицы, 108 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	Основные понятия и классификация криптографических протоколов	6	8	2	-	2	-	-	-	-	-	2	-	<p><b><u>Подготовка реферата:</u></b> Выбор темы реферата.</p> <p><b><u>Подготовка расчетных заданий:</u></b> Выбор темы расчетного задания.</p> <p><b><u>Подготовка к практическим занятиям:</u></b> Изучение материалов лекции 1 и литературы.</p> <p><b><u>Изучение материалов литературных источников:</u></b> [2], Глава 1 [5], Стр. 6-11 [6], Главы 1, 2 [8], Разд. 1, 3, 6, 9</p>		
1.1	Основные понятия и классификация криптографических протоколов	6		2	-	2	-	-	-	-	-	2	-			
2	Протоколы распределения ключей и аутентификации	24		10	4	4	-	-	-	-	-	-	6		-	<p><b><u>Подготовка к практическим занятиям:</u></b> Изучение материалов лекций 2-6 и литературы.</p> <p><b><u>Подготовка реферата:</u></b> Подбор источников по теме реферата.</p> <p><b><u>Подготовка расчетных заданий:</u></b> 1. Проектирование программы для расчетного задания. 2. Выбор языковых и инструментальных средств разработки.</p> <p><b><u>Подготовка к лабораторной работе:</u></b> Изучение задания на лабораторную работу 1.</p> <p><b><u>Подготовка к текущему контролю:</u></b> Тестирование и отладка программы для лабораторной работы 1.</p> <p><b><u>Изучение материалов литературных</u></b></p>
2.1	Протоколы распределения ключей и аутентификации	24		10	4	4	-	-	-	-	-	-	6		-	

													<b><u>источников:</u></b> [1], Разд. 1 [2], Глава 5 [4], Глава 2 [6], Разд. 3.1-3.3, 4.3, 6.3, 6.4. Глава 5 [7], Стр. 148-153
3	Протоколы разделения секрета, предсказания и голосования	20	10	2	4	-	-	-	-	-	4	-	<b><u>Подготовка к практическим занятиям:</u></b> Изучение материалов лекций 7-11 и литературы. <b><u>Подготовка реферата:</u></b> Подготовка доклада и компьютерной презентации для защиты реферата. <b><u>Подготовка расчетных заданий:</u></b> Разработка, тестирование и отладка программы для расчетного задания. <b><u>Подготовка к лабораторной работе:</u></b> Изучение задания на лабораторную работу 2. <b><u>Подготовка к текущему контролю:</u></b> Подготовка отчета о выполнении лабораторной работы 2. <b><u>Изучение материалов литературных источников:</u></b> [1], Разд. 2 [2], Глава 6 [4], Глава 3 [6], Разд. 3.6, 4.2, 4.8-4.11, 6.1, 6.2.
3.1	Протоколы разделения секрета, предсказания и голосования	20	10	2	4	-	-	-	-	-	4	-	<b><u>Подготовка к текущему контролю:</u></b> Тестирование и отладка программы для лабораторной работы 3. <b><u>Подготовка к лабораторной работе:</u></b> Изучение задания на лабораторную работу 3. <b><u>Подготовка расчетных заданий:</u></b> Подготовка отчета о выполнении расчетного задания. <b><u>Подготовка к практическим занятиям:</u></b> Изучение материалов лекций 12-14 и литературы. <b><u>Изучение материалов литературных источников:</u></b>
4	Криптографические методы в инфраструктуре открытых ключей	22	6	8	4	-	-	-	-	-	4	-	<b><u>Подготовка к текущему контролю:</u></b> Тестирование и отладка программы для лабораторной работы 3. <b><u>Подготовка к лабораторной работе:</u></b> Изучение задания на лабораторную работу 3. <b><u>Подготовка расчетных заданий:</u></b> Подготовка отчета о выполнении расчетного задания. <b><u>Подготовка к практическим занятиям:</u></b> Изучение материалов лекций 12-14 и литературы. <b><u>Изучение материалов литературных источников:</u></b>
4.1	Криптографические методы в инфраструктуре открытых ключей	22	6	8	4	-	-	-	-	-	4	-	<b><u>Подготовка к текущему контролю:</u></b> Тестирование и отладка программы для лабораторной работы 3. <b><u>Подготовка к лабораторной работе:</u></b> Изучение задания на лабораторную работу 3. <b><u>Подготовка расчетных заданий:</u></b> Подготовка отчета о выполнении расчетного задания. <b><u>Подготовка к практическим занятиям:</u></b> Изучение материалов лекций 12-14 и литературы. <b><u>Изучение материалов литературных источников:</u></b>

														[1], Разд. 3 [3], Разд. 2, 4 [5], Стр. 18-21, 27-29
	Экзамен	36.0		-	-	-	-	2	-	-	0.5	-	33.5	
	Всего за семестр	108.0		28	14	14	-	2	-	-	0.5	16	33.5	
	Итого за семестр	108.0		28	14	14	2		-		0.5	49.5		

**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. Основные понятия и классификация криптографических протоколов

##### 1.1. Основные понятия и классификация криптографических протоколов

Основные понятия современной криптографии. Понятие и классификация криптографических протоколов. Атаки на криптографические протоколы и методы их анализа..

#### 2. Протоколы распределения ключей и аутентификации

##### 2.1. Протоколы распределения ключей и аутентификации

Требования к распределению ключей и способы его реализации. Обмен ключами с помощью центра распределения ключей. Атака «человек посередине» и методы защиты от нее. Прямой обмен ключами. Протоколы Хьюза и обмена ключами с помощью посредника. Обновление сеансовых ключей и их передача вместе с сообщениями. Анонимное распределение ключей и обмен зашифрованными ключами. Депонирование ключей. Протоколы односторонней аутентификации. Протоколы взаимной аутентификации. Аутентификация сообщений. Аутентификация и обмен ключами. Протокол Нидхама-Шредера. Протоколы с нулевым разглашением. Протокол Шнорра. Протоколы Фиата-Шамира и Фейге-Фиата-Шамира. Протокол Гиллоу-Куискуотера. Получение нескольких электронных подписей (ЭП) под одним документом. Неоспоримая и не отрицаемая ЭП. ЭП вслепую..

#### 3. Протоколы разделения секрета, предсказания и голосования

##### 3.1. Протоколы разделения секрета, предсказания и голосования

Протоколы разделения секрета. Мошенничество при разделении секрета и защита от него. Подсознательный канал. Электронная почта с подтверждением. Одновременное подписание контракта. Предсказание бита. Электронное бросание монеты. Компьютерный покер. Вычисления с секретными данными. Задача «миллионеров». Безопасные вычисления с несколькими участниками. Простые протоколы электронного голосования. Голосование со слепыми подписями. Голосование с центральной избирательной комиссией. Голосование без центральной избирательной комиссии..

#### 4. Криптографические методы в инфраструктуре открытых ключей

##### 4.1. Криптографические методы в инфраструктуре открытых ключей

Элементы инфраструктуры открытых ключей (Public Key Infrastructure, PKI). Архитектура PKI. Распространение сертификатов и списков отозванных сертификатов (Certificate Revocation List, CRL). Управление жизненным циклом сертификатов. Способы хранения личных (закрытых) ключей пользователей PKI..

### **3.3. Темы практических занятий**

1. Способы хранения личных ключей;
2. Инфраструктура открытых ключей: ее элементы, архитектура удостоверяющих центров, способы распространения и отзыва сертификатов;
3. Протоколы разделения секрета и электронного голосования;
4. Протоколы вычислений с секретными данными;
5. Протоколы с нулевым разглашением информации;
6. Протоколы распределения криптографических ключей;
7. Основные понятия криптографических протоколов, их классификация и методы

анализа.

### **3.4. Темы лабораторных работ**

1. Средства использования сертификатов открытых ключей;
2. Запрос и получение сертификатов открытых ключей в удостоверяющем центре;
3. Средства создания и проверки электронной подписи.

### **3.5 Консультации**

#### *Групповые консультации по разделам дисциплины (ГК)*

1. Консультирование по вопросам выбора тем реферата и расчетного задания.
2. Консультирование по материалам лекций 2-6.
3. Консультирование по материалам лекций 7-11.
4. Консультирование по материалам лекций 12-14.

#### *Текущий контроль (ТК)*

1. Консультирование по порядку защиты лабораторной работы 1.
2. Консультирование по защите реферата и лабораторной работы 2.
3. Консультирование по защите лабораторной работы 3 и расчетного задания.

### **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	
<b>Знать:</b>						
Особенности использования криптографических методов защиты информации при решении различных прикладных задач	ИД-1ПК-3			+		Лабораторная работа/Выполнение и защита лабораторной работы 2; защита реферата
Способы построения симметричных и асимметричных криптографических систем	ИД-1ПК-3	+				Тестирование/Тест по разделу 1
Современные технологии создания программных средств криптографической защиты информации	ИД-1ПК-3				+	Лабораторная работа/Выполнение и защита лабораторной работы 3; защита расчетного задания
Способы управления криптографическими ключами и сертификатами открытых ключей;	ИД-1ПК-3		+			Лабораторная работа/Выполнение и защита лабораторной работы 1
Достоинства и недостатки современных криптографических систем	ИД-2ПК-3	+				Тестирование/Тест по разделу 1
Российские и международные стандарты в области криптографических алгоритмов и протоколов	ИД-2ПК-3				+	Лабораторная работа/Выполнение и защита лабораторной работы 3; защита расчетного задания
Тенденции развития криптографических методов защиты информации	ИД-2ПК-3				+	Лабораторная работа/Выполнение и защита лабораторной работы 3; защита расчетного задания
<b>Уметь:</b>						
Использовать методы и средства криптографической защиты информации для создания защищенного электронного документооборота	ИД-1ПК-3				+	Лабораторная работа/Выполнение и защита лабораторной работы 3; защита расчетного задания
Предлагать методы и средства повышения информационной безопасности компьютерных систем и сетей, основанные на криптографической защите информации	ИД-1ПК-3				+	Лабораторная работа/Выполнение и защита лабораторной работы 3; защита расчетного задания

Использовать методы и средства криптографической защиты информации при обеспечении информационной безопасности компьютерных систем и сетей	ИД-1ПК-3			+		Лабораторная работа/Выполнение и защита лабораторной работы 2; защита реферата
Анализировать эффективность используемых криптографических методов и средств защиты информации	ИД-2ПК-3			+		Лабораторная работа/Выполнение и защита лабораторной работы 1
Определять цели и задачи разработки новых методов и программных средств криптографической защиты информации в компьютерных системах и сетях	ИД-2ПК-3				+	Лабораторная работа/Выполнение и защита лабораторной работы 3; защита расчетного задания
Использовать литературу и источники сети Интернет для получения информации о создании новых криптографических методов и средств защиты информации	ИД-2ПК-3				+	Лабораторная работа/Выполнение и защита лабораторной работы 3; защита расчетного задания
Разрабатывать новые безопасные информационные технологии с использованием криптографических методов и средств	ИД-2ПК-3			+		Лабораторная работа/Выполнение и защита лабораторной работы 2; защита реферата

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

### **4.1. Текущий контроль успеваемости**

**8 семестр**

Форма реализации: Компьютерное задание

1. Выполнение и защита лабораторной работы 1 (Лабораторная работа)
2. Выполнение и защита лабораторной работы 3; защита расчетного задания (Лабораторная работа)

Форма реализации: Письменная работа

1. Тест по разделу 1 (Тестирование)

Форма реализации: Смешанная форма

1. Выполнение и защита лабораторной работы 2; защита реферата (Лабораторная работа)

Балльно-рейтинговая структура дисциплины является приложением А.

### **4.2 Промежуточная аттестация по дисциплине**

*Экзамен (Семестр №8)*

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 8 семестр.

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

## **5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ**

### **5.1 Печатные и электронные издания:**

1. Хорев, П. Б. Криптографические протоколы : учебное пособие по курсу "Криптографические методы защиты информации" по направлению 01.03.02 "Прикладная математика и информатика" / П. Б. Хорев, Нац. исслед. ун-т "МЭИ" (НИУ"МЭИ"). – М. : Изд-во МЭИ, 2019. – 88 с. – ISBN 978-5-7046-2162-1.  
<http://elibr.mpei.ru/elibr/view.php?id=10969>;
2. Черемушкин, А. В. Криптографические протоколы. Основные свойства и уязвимости : учебное пособие для вузов по специальности "Компьютерная безопасность" / А. В. Черемушкин. – М. : АКАДЕМИЯ, 2010. – 272 с. – (Высшее профессиональное образование). – ISBN 978-5-7695-5748-4.;
3. Горбатов, В. С. Основы технологии РКК / В. С. Горбатов, О. Ю. Полянская. – М. : Горячая Линия-Телеком, 2004. – 248 с. – ISBN 5-935171-54-6.;
4. Хорев, П. Б. Использование средств шифрования данных в приложениях для Microsoft.Net : учебное пособие по курсу "Защита данных" по направлению "Прикладная математика и информатика" / П. Б. Хорев, Нац. исслед. ун-т "МЭИ". – М. : Изд-во МЭИ, 2015. – 92 с. – ISBN 978-5-7046-1665-8.  
<http://elibr.mpei.ru/elibr/view.php?id=8104>;
5. Хорев, П. Б. Криптографические методы защиты информации : практикум по курсу "Криптографические методы защиты информации" по направлению 01.03.02 "Прикладная

математика и информатика" / П. Б. Хорев, Нац. исслед. ун-т "МЭИ" (НИУ"МЭИ"). – Москва : Изд-во МЭИ, 2020. – 52 с. – ISBN 978-5-7046-2321-2.

<http://elibr.mpei.ru/elibr/view.php?id=11319>;

6. Шнайер, Б. Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си : пер. с англ. / Б. Шнайер. – М. : Триумф, 2002. – 816 с. – ISBN 5-89392-055-4.;

7. Романец, Ю. В. Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин. – М. : Радио и связь, 1999. – 328 с. – ISBN 5-256-01436-6 : 53.00.;

8. Басалова Г. В.- "Основы криптографии", (2-е изд.), Издательство: "ИНТУИТ", Москва, 2016 - (282 с.)

<https://e.lanbook.com/book/100302>.

## **5.2 Лицензионное и свободно распространяемое программное обеспечение:**

1. СДО "Прометей";

2. Office / Российский пакет офисных программ;

3. Windows / Операционная система семейства Linux;

4. Видеоконференции (Майнд, Сберджаз, ВК и др);

5. Windows Server / Серверная операционная система семейства Linux;

6. Visual Studio.

## **5.3 Интернет-ресурсы, включая профессиональные базы данных и информационно-справочные системы:**

1. ЭБС Лань - <https://e.lanbook.com/>

2. Национальная электронная библиотека - <https://rusneb.ru/>

3. База данных Computers & Applied Sciences Complete (CASC) -

<http://search.ebscohost.com>

4. Электронная библиотека МЭИ (ЭБ МЭИ) - <http://elibr.mpei.ru/login.php>

5. Портал открытых данных Российской Федерации - <https://data.gov.ru>

6. База открытых данных профессиональных стандартов Министерства труда и социальной защиты РФ - <http://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/>

7. Информационно-справочная система «Кодекс/Техэксперт» - <Http://proinfosoft.ru>;  
<http://docs.cntd.ru/>

8. Национальный портал онлайн обучения «Открытое образование» - <https://openedu.ru>

## **6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ**

Тип помещения	Номер аудитории, наименование	Оснащение
Учебные аудитории для проведения лекционных занятий и текущего контроля	М-805, Учебная аудитория каф. "ПМИИ"	парта со скамьей, доска меловая, компьютерная сеть с выходом в Интернет, мультимедийный проектор, экран, компьютер персональный
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
Учебные аудитории для проведения практических занятий, КР и КП	М-912, Учебная аудитория	кресло рабочее, стол преподавателя, стол учебный, стул, доска интерактивная, компьютерная сеть с выходом в Интернет, доска маркерная
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
Учебные аудитории для	М-708, Дисплейный	стол преподавателя, стол

проведения лабораторных занятий	класс каф. "ПМИИ"	компьютерный, стул, компьютерная сеть с выходом в Интернет, мультимедийный проектор, экран, компьютер персональный, кондиционер
Учебные аудитории для проведения промежуточной аттестации	М-708, Дисплейный класс каф. "ПМИИ"	стол преподавателя, стол компьютерный, стул, компьютерная сеть с выходом в Интернет, мультимедийный проектор, экран, компьютер персональный, кондиционер
Помещения для самостоятельной работы	НТБ-303, Лекционная аудитория	стол компьютерный, стул, стол письменный, вешалка для одежды, компьютерная сеть с выходом в Интернет, компьютер персональный, принтер, кондиционер
Помещения для консультирования	М-704, Преподавательская кафедры ПМИИ	стол, стул, шкаф, тумба, доска меловая, компьютерная сеть с выходом в Интернет, мультимедийный проектор, экран, компьютер персональный, холодильник, кондиционер
Помещения для хранения оборудования и учебного инвентаря	М-703а/1, Кладовая каф. "ПМИИ"	стеллаж для хранения книг, тумба, экран, ноутбук, книги, учебники, пособия

## БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

### Криптографические методы защиты информации

(название дисциплины)

#### 8 семестр

#### Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

КМ-1 Тест по разделу 1 (Тестирование)

КМ-2 Выполнение и защита лабораторной работы 1 (Лабораторная работа)

КМ-3 Выполнение и защита лабораторной работы 2; защита реферата (Лабораторная работа)

КМ-4 Выполнение и защита лабораторной работы 3; защита расчетного задания (Лабораторная работа)

#### Вид промежуточной аттестации – Экзамен.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
		Неделя КМ:	4	7	11	14
1	Основные понятия и классификация криптографических протоколов					
1.1	Основные понятия и классификация криптографических протоколов		+			
2	Протоколы распределения ключей и аутентификации					
2.1	Протоколы распределения ключей и аутентификации			+		
3	Протоколы разделения секрета, предсказания и голосования					
3.1	Протоколы разделения секрета, предсказания и голосования			+	+	
4	Криптографические методы в инфраструктуре открытых ключей					
4.1	Криптографические методы в инфраструктуре открытых ключей					+
Вес КМ, %:			20	25	25	30