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

Направление подготовки/специальность: 10.03.01 Информационная безопасность

Наименование образовательной программы: Безопасность компьютерных систем

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

Рабочая программа дисциплины
МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Обязательная**
№ дисциплины по учебному плану:	**Б1.О.29**
Трудоемкость в зачетных единицах:	**5 семестр - 4;**
Часов (всего) по учебному плану:	**144 часа**
Лекции	**5 семестр - 32 часа;**
Практические занятия	**5 семестр - 32 часа;**
Лабораторные работы	**не предусмотрено учебным планом**
Консультации	**5 семестр - 2 часа;**
Самостоятельная работа	**5 семестр - 77,5 часа;**
в том числе на КП/КР	**не предусмотрено учебным планом**
Иная контактная работа	**проводится в рамках часов аудиторных занятий**
включая: **Домашнее задание** **Контрольная работа** **Реферат**	
Промежуточная аттестация:	
Экзамен	**5 семестр - 0,5 часа;**

Москва 2023

ПРОГРАММУ СОСТАВИЛ:

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

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Баронов О.Р. Идентификатор: R90d76356-BaronovOR-7bf8fd7e	О.Р. Баронов
Заведующий выпускающей кафедрой	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d	А.Ю. Невский

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины: изучение современных методов синтеза криптосистем и криптопротоколов, а также методов их анализа для обеспечения эффективной криптографической защиты информации

Задачи дисциплины

- освоение методов и приобретения навыков обеспечения конфиденциальности на основе математических методов преобразования информации;
- освоение методов и приобретения навыков обеспечения целостности на основе математических методов преобразования информации;
- освоение методов и приобретения навыков обеспечения аутентификации на основе математических методов преобразования информации;
- освоение методов и приобретения навыков обеспечения невозможности отказа (от авторства) на основе математических методов преобразования информации;
- освоение методов и приобретения навыков обеспечения неотслеживаемости на основе математических методов преобразования информации.

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

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Запланированные результаты обучения**
ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ИД-1$_{ОПК-9}$ Настраивает программные и аппаратные средства построения компьютерных сетей, использующих криптографическую защиту информации	знать: - методы обеспечения конфиденциальности, целостности информации, подлинности сторон информационного взаимодействия, невозможности отказа от авторства, неотслеживаемости; - принципы построения современных криптосистем и криптопротоколов. уметь: - применять методы обеспечения конфиденциальности, целостности, подтверждения подлинности, невозможности отказа от авторства, неотслеживаемости; - использовать принципы построения современных криптосистем и криптопротоколов; - формулировать и решать задачи построения защищенных профессионально-ориентированных автоматизированных систем с использованием криптографических методов.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к основной профессиональной образовательной программе Безопасность компьютерных систем (далее – ОПОП), направления подготовки 10.03.01 Информационная безопасность, уровень образования: высшее образование - бакалавриат.

Базируется на уровне среднего общего образования.

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

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы, 144 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	Основы криптографической защиты информации	26	5	6	-	8	-	-	-	-	-	12	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Основы криптографической защиты информации" ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Основы криптографической защиты информации" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. ***Подготовка доклада, выступления:*** Задание связано с углубленным изучением разделов дисциплины и самостоятельным поиском материалов для раскрытия темы доклада. Материалы выполненной работы представляются в электронном виде или в форме распечатанных презентационных слайдов. В качестве тем докладов студентам предлагаются следующие варианты: ***Подготовка к контрольной работе:***
1.1	Место криптографической защиты информации в обеспечении информационной безопасности	8		2	-	2	-	-	-	-	-	4	-	
1.2	Тема 1. Основные понятия криптографической защиты информации	8		2	-	2	-	-	-	-	-	4	-	
1.3	Тема 2. Основы криптографических методов защиты информации	10		2	-	4	-	-	-	-	-	4	-	

														Изучение материалов по разделу Основы криптографической защиты информации и подготовка к контрольной работе ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Основы криптографической защиты информации" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Основы криптографической защиты информации" ***Подготовка реферата:*** В рамках реферативной части студенту необходим провести обзор литературных источников по выбранной теме, комплексно осветить вопрос в соответствии с темой реферата, подготовить презентацию для выступления по результатам работы на семинарском занятии. В качестве тем реферата студенту предлагаются следующие варианты: ***Изучение материалов литературных источников:*** [1], 1-528 [4], 1-232
2	Симметричные и асимметричные криптосистемы, средства их реализации	40		12	-	12	-	-	-	-	-	16	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Симметричные и асимметричные криптосистемы, средства их реализации" ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Симметричные и асимметричные
2.1	Тема 3. Симметричные блочные шифры	8		2	-	2	-	-	-	-	-	4	-	
2.2	Тема 4. Поточные шифры	8		2	-	2	-	-	-	-	-	4	-	
2.3	Тема 5. Концепция криптосистем с открытыми ключами	12		4	-	4	-	-	-	-	-	4	-	

	и ее реализация на базе модулярной арифметики и эллиптических кривых													криптосистемы, средства их реализации" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. ***Подготовка доклада, выступления:*** Задание связано с углубленным изучением разделов дисциплины и самостоятельным поиском материалов для раскрытия темы доклада. Материалы выполненной работы представляются в электронном виде или в форме распечатанных презентационных слайдов. В качестве тем докладов студентам предлагаются следующие варианты: ***Подготовка к контрольной работе:*** Изучение материалов по разделу Симметричные и асимметричные криптосистемы, средства их реализации и подготовка к контрольной работе ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Симметричные и асимметричные криптосистемы, средства их реализации" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Симметричные и асимметричные криптосистемы, средства их реализации" ***Подготовка реферата:*** В рамках реферативной части студенту необходим провести обзор литературных источников по выбранной теме, комплексно осветить вопрос в соответствии с темой реферата, подготовить презентацию для выступления по результатам работы на семинарском занятии. В качестве тем реферата студенту предлагаются следующие варианты:
2.4	Тема 6. Нормативно-правовые акты криптографической защиты информации	12		4	-	4	-	-	-	-	-	4	-	

														Изучение материалов литературных источников: [2], 1-328 [5], 1-136 [7], 1-257 [9], стр. 12-40
3	Криптографические протоколы, хэш-функции, электронные подписи средства их реализации	42		14	-	12	-	-	-	-	-	16	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Криптографические протоколы, хэш-функции, электронные подписи средства их реализации" ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Криптографические протоколы, хэш-функции, электронные подписи средства их реализации" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. ***Подготовка доклада, выступления:*** Задание связано с углубленным изучением разделов дисциплины и самостоятельным поиском материалов для раскрытия темы доклада. Материалы выполненной работы представляются в электронном виде или в форме распечатанных презентационных слайдов. В качестве тем докладов студентам предлагаются следующие варианты: ***Подготовка к контрольной работе:*** Изучение материалов по разделу Криптографические протоколы, хэш-
3.1	Тема 7. Криптографические протоколы	20		6	-	6	-	-	-	-	-	8	-	
3.2	Тема 8. Хэш-функции и электронные подписи	22		8	-	6	-	-	-	-	-	8	-	

														функции, электронные подписи средства их реализации и подготовка к контрольной работе ***<u>Подготовка к практическим занятиям:</u>*** Изучение материала по разделу "Криптографические протоколы, хэш-функции, электронные подписи средства их реализации" подготовка к выполнению заданий на практических занятиях ***<u>Самостоятельное изучение теоретического материала:</u>*** Изучение дополнительного материала по разделу "Криптографические протоколы, хэш-функции, электронные подписи средства их реализации" ***<u>Подготовка реферата:</u>*** В рамках реферативной части студенту необходим провести обзор литературных источников по выбранной теме, комплексно осветить вопрос в соответствии с темой реферата, подготовить презентацию для выступления по результатам работы на семинарском занятии. В качестве тем реферата студенту предлагаются следующие варианты: ***<u>Изучение материалов литературных источников:</u>*** [3], 1-512 [6], 1-200 [8], 1-209 [9], стр. 52-95
	Экзамен	36.0		-	-	-	-	2	-	-	0.5	-	33.5	
	Всего за семестр	**144.0**		**32**	**-**	**32**	**-**	**2**	**-**	**-**	**0.5**	**44**	**33.5**	
	Итого за семестр	**144.0**		**32**	**-**	**32**	**2**		**-**		**0.5**	**77.5**		

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. Основы криптографической защиты информации

1.1. Место криптографической защиты информации в обеспечении информационной безопасности

Предмет, цели, задачи, содержание и структура дисциплины криптографические методы защиты информации (КМЗИ). Базовые знания, необходимые для изучения курса. Рекомендуемые учебные пособия по дисциплине..

1.2. Тема 1. Основные понятия криптографической защиты информации

Особенности задач криптографической защиты информации. Понятие шифра и примеры шифров: шифры замены, перестановки, гаммирования. Требования к шифрам. Теоретическая стойкость шифров. Совершенно стойкие шифры. Практическая стойкость шифров и подходы к ее оценке. Атаки на шифры. Понятие о криптографических протоколах. Криптосистемы и их виды..

1.3. Тема 2. Основы криптографических методов защиты информации

Математические модели шифров. Ключевая система шифра. Элементы математической теории информации. Модели открытых текстов и подходы к распознаванию открытого текста. Энтропии шифртекстов и ключей. Расстояние единственности шифра. Конечные автоматы, их функционирование, виды, способы задания, отношения и операции с ними. Шифрующие автоматы. Автоматные модели шифров. Псевдослучайные последовательности. Подходы к анализу этих последовательностей, требования к ним и тестирование. Линейные рекуррентные последовательности (ЛРП) и их реализация на линейных регистрах сдвига (ЛРС). Линейная сложность последовательности. Алгоритм Берлекемпа-Месси. Криптографические генераторы и их виды..

2. Симметричные и асимметричные криптосистемы, средства их реализации

2.1. Тема 3. Симметричные блочные шифры

Принципы построения блочных шифров. Американский стандарт шифрования данных DES. Отечественный стандарт шифрования данных. Стандарт шифрования данных AES. Режимы использования блочных шифров. Методы анализа алгоритмов блочного шифрования. Рекомендации по использованию алгоритмов блочного шифрования. Алгоритмы «облегченной» (lightweight) криптографии и области их применения..

2.2. Тема 4. Поточные шифры

Вопросы синхронизации поточных систем шифрования. Синхронные и асинхронные системы. Принципы построения поточных криптосистем, примеры криптосистем. Элементы криптоанализа поточных шифров..

2.3. Тема 5. Концепция криптосистем с открытыми ключами и ее реализация на базе модулярной арифметики и эллиптических кривых

Принципы построения криптосистем с открытым ключом. Однонаправленные функции. Особенности использования асимметричных криптосистем. Шифрсистема RSA, возможные атаки на нее. Шифрсистема Эль-Гамаля. Кодирование и шифрование, шифрсистема Мак-Элиса. Шифрсистема Полига-Хеллмана. Криптосистемы на эллиптических кривых..

2.4. Тема 6. Нормативно-правовые акты криптографической защиты информации

Классификация средств криптографической защиты информации. Средства защиты информации на персональном компьютере..

3. Криптографические протоколы, хэш-функции, электронные подписи средства их реализации

3.1. Тема 7. Криптографические протоколы

Понятие криптографического протокола. Идентификация и аутентификация пользователей. Протоколы распределение ключей с использованием симметричного и асимметричного шифрования. Открытое распределение ключей. Предварительное распределение ключей. Атаки на протоколы распределения ключей. Криптографические протоколы на эллиптических кривых..

3.2. Тема 8. Хэш-функции и электронные подписи

Понятие хэш-функций и их предназначение. Типы хэш-функций и требования к ним. Реализация хэш-функций с помощью блочных шифров. Однонаправленные хэш-функции. Атаки на хэш-функции. Стандарты на хэш-функции. Понятие электронной подписи и ее использование. Подходы к созданию схем электронной подписи. Целостность данных и аутентификация сообщений. Алгоритм электронной подписи RSA. Алгоритм электронной подписи Эль-Гамаля. Алгоритм электронной подписи DSA. Стандарты на электронные подписи. Средства криптографической защиты сетевого взаимодействия..

3.3. Темы практических занятий

1. 11. Криптографические протоколы. Примеры протоколов идентификации и аутентификации пользователей и криптопротоколов на эллиптических кривых;
2. 13. Электронные подписи. Примеры реализации алгоритмов электронной подписи RSA, Эль – Гамаля и DSA. Отечественный стандарт на электронную подпись;
3. 14. Нормативно-правовая база криптографической защиты информации;
4. 2. Элементы криптоанализа шифров простой замены, шифров перестановки и шифров гаммирования;
5. 9. Поточные шифры. Примеры реализации синхронных и асинхронных шифров;
6. 4. Линейная сложность последовательности и ее определение посредством использования алгоритма Берлекемпа - Месси;
7. 12. Хэш-функции. Реализация хэш-функций с помощью блочных шифров и специальных алгоритмов. Отечественный стандарт на хэш-функции;
8. 6. Симметричные блочные шифры. Стандарт шифрования данных DES. Реализация пре-образований петли Фейстеля. Генерирование раундовых ключей;
9. 15. Аппаратные и программные средства криптографической защиты информации;
10. 5. Криптографические генераторы и их виды. Фильтрующие генераторы. Комбинирующие генераторы. Генераторы гаммы с неравномерным движением. Генераторы с дополнительной памятью;
11. 8. Симметричные блочные шифры. Реализация операций отечественного стандарта шифрования данных;
12. 1. Понятие шифра и примеры шифров: поточные шифры простой замены, маршрутные перестановки, табличное гаммирование;
13. 7. Симметричные блочные шифры. Стандарт шифрования данных AES. Реализация вычислений в конечных полях Галуа GF(28). Реализация операции BS. Обработка четырех-байтовых массивов (слов);
14. 3. Псевдослучайные последовательности. Подходы к анализу этих последовательностей, требования к ним и тестирование. Линейные рекуррентные последовательности (ЛРП) и их реализация на линейных регистрах сдвига (ЛРС);

15. 10. Асимметричные шифрсистемы. Реализация расширенного алгоритма Евклида и его модификации в виде метода Гаусса. Реализация шифрсистемы RSA.

3.4. Темы лабораторных работ

не предусмотрено

3.5 Консультации

Групповые консультации по разделам дисциплины (ГК)

1. Обсуждение материалов по кейсам раздела "Основы криптографической защиты информации"
2. Обсуждение материалов по кейсам раздела "Симметричные и асимметричные криптосистемы, средства их реализации"
3. Обсуждение материалов по кейсам раздела "Криптографические протоколы, хэш-функции, электронные подписи средства их реализации"

Текущий контроль (ТК)

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Основы криптографической защиты информации"
2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Симметричные и асимметричные криптосистемы, средства их реализации"
3. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Криптографические протоколы, хэш-функции, электронные подписи средства их реализации"

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	
Знать:					
принципы построения современных криптосистем и криптопротоколов	ИД-1$_{ОПК-9}$	+			Домашнее задание/Защита домашнего задания «Дешифрование классических шифров» Реферат/Защита реферата
методы обеспечения конфиденциальности, целостности информации, подлинности сторон информационного взаимодействия, невозможности отказа от авторства, неотслеживаемости	ИД-1$_{ОПК-9}$		+		Реферат/Защита реферата Контрольная работа/Контрольная работа №1 «Симметричные и асимметричные криптосистемы»
Уметь:					
формулировать и решать задачи построения защищенных профессионально-ориентированных автоматизированных систем с использованием криптографических методов	ИД-1$_{ОПК-9}$		+		Контрольная работа/Контрольная работа №1 «Симметричные и асимметричные криптосистемы»
использовать принципы построения современных криптосистем и криптопротоколов	ИД-1$_{ОПК-9}$			+	Контрольная работа/Контрольная работа №2. «Криптографические протоколы, хэш-функции и электронные подписи»
применять методы обеспечения конфиденциальности, целостности, подтверждения подлинности, невозможности отказа от авторства, неотслеживаемости	ИД-1$_{ОПК-9}$			+	Реферат/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

5 семестр

Форма реализации: Защита задания

1. Защита домашнего задания «Дешифрование классических шифров» (Домашнее задание)
2. Защита реферата (Реферат)

Форма реализации: Письменная работа

1. Контрольная работа №1 «Симметричные и асимметричные криптосистемы» (Контрольная работа)
2. Контрольная работа №2. «Криптографические протоколы, хэш-функции и электронные подписи» (Контрольная работа)

Балльно-рейтинговая структура дисциплины является приложением А.

4.2 Промежуточная аттестация по дисциплине

Экзамен (Семестр №5)

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

В диплом выставляется оценка за 5 семестр.

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

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Печатные и электронные издания:

1. Смарт, Н. Криптография : пер. с англ. / Н. Смарт . – М. : Техносфера, 2005 . – 528 с. – (Мир программирования) . - ISBN 5-948360-43-1 .;
2. Болотов, А. А. Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых / А. А. Болотов, С. Б. Гашков, А. Б. Фролов . – 2006 . – 280 с. - ISBN 5-484-00444-6 .;
3. Бабаш, А. В. Криптография / А. В. Бабаш, Г. П. Шанкин ; Ред. В. П. Шерстюк, Э. А. Применко . – М. : Солон-Пресс, 2007 . – 512 с. – (Аспекты защиты) . - ISBN 5-934551-35-3 .;
4. Рябко, Б. Я. Основы современной криптографии и стенографии / Б. Я. Рябко, А. Н. Фионов . – М. : Горячая Линия-Телеком, 2010 . – 232 с. - ISBN 978-5-9912-0150-6 .;
5. Бабаш, А. В. Информационная безопасность: лабораторный практикум : учебное пособие / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников . – 2-е изд., стереотип . – М. : КноРус, 2013 . – 136 с. + CD . – (Бакалавриат) . - ISBN 978-5-406-02760-8 .;
6. Жданов, О. Н. Эллиптические кривые. Основы теории и криптографические приложения / О. Н. Жданов, В. А. Чалкин, Сиб. аэрокосмическая акад. им. М.Ф. Решетнева . – М. : Эдиториал УРСС, 2013 . – 200 с. – (Основы защиты информации) . - ISBN 978-5-397-03230-8 .;

7. Бабаш, А. В. Криптографические методы защиты информации. Т.3 : учебно-методическое пособие по специальности 080801 "Прикладная информатика" и другим междисциплинарным специальностям / А. В. Бабаш . – 2-е изд . – М. : РИОР : ИНФРА-М, 2014 . – 216 с. – (Высшее образование . Бакалавриат) . - ISBN 978-5-369-01304-5 .;
8. Фомичев, В. М. Криптографические методы защиты информации: [в 2 ч.]. Ч. 1.: Математические аспекты : учебник для академического бакалавриата вузов по инженерно-техническим направлениям / В. М. Фомичев, Д. А. Мельников ; ред. В. М. Фомичев . – М. : Юрайт, 2018 . – 209 с. – (Бакалавр. Академический курс) . - ISBN 978-5-9916-7089-0 . - ISBN 978-5-9916-7088-3 .;
9. Рябко Б. Я., Фионов А. Н.- "Криптографические методы защиты информации", (2-е изд., стер.), Издательство: "Горячая линия-Телеком", Москва, 2017 - (230 с.) https://e.lanbook.com/book/111097.

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).

5.3 Интернет-ресурсы, включая профессиональные базы данных и информационно-справочные системы:
1. **ЭБС Лань** - https://e.lanbook.com/
2. **ЭБС "Университетская библиотека онлайн"** - http://biblioclub.ru/index.php?page=main_ub_red
3. **Научная электронная библиотека** - https://elibrary.ru/
4. **База данных Web of Science** - http://webofscience.com/
5. **База данных Scopus** - http://www.scopus.com
6. **ЭБС "Консультант студента"** - http://www.studentlibrary.ru/
7. **Электронная библиотека МЭИ (ЭБ МЭИ)** - http://elib.mpei.ru/login.php
8. **Портал открытых данных Российской Федерации** - https://data.gov.ru
9. **База открытых данных Министерства труда и социальной защиты РФ** - https://rosmintrud.ru/opendata
10. **Открытая университетская информационная система «РОССИЯ»** - https://uisrussia.msu.ru

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Тип помещения	Номер аудитории, наименование	Оснащение
Учебные аудитории для проведения лекционных занятий и текущего контроля	Н-204, Учебная аудитория	парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, колонки звуковые, мультимедийный проектор, экран
	К-601, Учебная аудитория	парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, мультимедийный проектор, экран
Учебные аудитории для проведения практических занятий, КР и КП	М-510, Учебная лаборатория информационно-аналитический технологий - компьютерный класс	стул, стол письменный, мультимедийный проектор, экран, доска маркерная, компьютер персональный, кондиционер

Учебные аудитории для проведения промежуточной аттестации	М-510, Учебная лаборатория информационно-аналитический технологий - компьютерный класс	стул, стол письменный, мультимедийный проектор, экран, доска маркерная, компьютер персональный, кондиционер
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
Помещения для самостоятельной работы	НТБ-201, Компьютерный читальный зал	стол компьютерный, стул, стол письменный, вешалка для одежды, компьютерная сеть с выходом в Интернет, компьютер персональный, принтер, кондиционер
Помещения для консультирования	А-300, Учебная аудитория "А"	кресло рабочее, парта, стеллаж, стол преподавателя, стол учебный, стул, трибуна, микрофон, мультимедийный проектор, экран, доска маркерная, колонки, техническая аппаратура, кондиционер, телевизор
Помещения для хранения оборудования и учебного инвентаря	К-202/2, Склад кафедры БИТ	стеллаж для хранения инвентаря, стол, стул, шкаф для документов, шкаф для хранения инвентаря, тумба, запасные комплектующие для оборудования

Приложение А

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Методы и средства криптографической защиты информации

(название дисциплины)

5 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

КМ-1 Защита домашнего задания «Дешифрование классических шифров» (Домашнее задание)

КМ-2 Контрольная работа №1 «Симметричные и асимметричные криптосистемы» (Контрольная работа)

КМ-3 Контрольная работа №2. «Криптографические протоколы, хэш-функции и электронные подписи» (Контрольная работа)

КМ-4 Защита реферата (Реферат)

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	Основы криптографической защиты информации					
1.1	Место криптографической защиты информации в обеспечении информационной безопасности		+			+
1.2	Тема 1. Основные понятия криптографической защиты информации		+			+
1.3	Тема 2. Основы криптографических методов защиты информации		+			+
2	Симметричные и асимметричные криптосистемы, средства их реализации					
2.1	Тема 3. Симметричные блочные шифры			+		+
2.2	Тема 4. Поточные шифры			+		+
2.3	Тема 5. Концепция криптосистем с открытыми ключами и ее реализация на базе модулярной арифметики и эллиптических кривых			+		+
2.4	Тема 6. Нормативно-правовые акты криптографической защиты информации			+		+
3	Криптографические протоколы, хэш-функции, электронные подписи средства их реализации					
3.1	Тема 7. Криптографические протоколы				+	+
3.2	Тема 8. Хэш-функции и электронные подписи				+	+
		Вес КМ, %:	25	25	25	25