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
КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Базовая**
№ дисциплины по учебному плану:	**Б1.Б.26**
Трудоемкость в зачетных единицах:	**6 семестр - 4;**
Часов (всего) по учебному плану:	**144 часа**
Лекции	**6 семестр - 14 часов;**
Практические занятия	**6 семестр - 28 часа;**
Лабораторные работы	**6 семестр - 14 часов;**
Консультации	**6 семестр - 2 часа;**
Самостоятельная работа	**6 семестр - 85,5 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	**6 семестр - 0,5 часа;**

Москва 2018

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
(должность)	(подпись)	(расшифровка подписи)

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
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)
Заведующий выпускающей кафедры	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d	А.Ю. Невский
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

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

Задачи дисциплины

- конфиденциальность;
- целостность;
- аутентификация;
- невозможность отказа (от авторства);
- неотслеживаемость.

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 способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации		знать: - действующую классификацию средств криптографической защиты информации. уметь: - пользоваться стандартными математическими методами при анализе криптографических алгоритмов.
ПК-4 способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты		знать: - сущность системного подхода к защите информации; - состояние нормативно-законодательной базы и стандарты в области криптографической защиты информации. уметь: - формулировать и решать задачи проектирования защищенных профессионально-ориентированных автоматизированных систем с использованием криптографических методов.
ОК-5 способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения		знать: - классификацию, требования к шифрам и основные характеристики шифров. уметь: - применять на практике положения законов РФ и ведомственных нормативных актов в области защиты информации.

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения
информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики		
ПСК-2 Способность применять программные средства системного и специального назначения, в том числе для обеспечения безопасносго функционирования объектов энергетики с элементами АСУ ТП		знать: - принципы построения современных криптосистем и криптопротоколов. уметь: - применять криптографические методы защиты информации в различных предметных областях.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к обязательной части блока дисциплин 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	РАЗДЕЛ 1. Основы криптографической защиты информации.	22	6	4	4	4	-	-	-	-	-	10	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "РАЗДЕЛ 1. 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 "РАЗДЕЛ 1. 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 к практическим занятиям:*** Изучение материала по разделу "РАЗДЕЛ 1. Основы криптографической защиты информации." подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "РАЗДЕЛ 1. Основы криптографической
1.1	Введение	3		1	-	-	-	-	-	-	-	2	-	
1.2	Тема 1. Основные понятия криптографической защиты информации	7		1	2	2	-	-	-	-	-	2	-	
1.3	Тема 2. Основы криптографических методов защиты информации	12		2	2	2	-	-	-	-	-	6	-	

														защиты информации." ***Изучение материалов литературных источников:*** [6], 1-232 [7], 1-528
2	РАЗДЕЛ 2. Симметричные и асиммтетричные шифрсистемы.	52		6	6	14	-	-	-	-	-	26	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "РАЗДЕЛ 2. Симметричные и асиммтетричные шифрсистемы."
2.1	Тема 3. Симметричные блочные шифры.	20		2	2	6	-	-	-	-	-	10	-	***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы
2.2	Тема 4. Поточные шифры.	16		2	2	4	-	-	-	-	-	8	-	***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "РАЗДЕЛ 2. Симметричные и асиммтетричные шифрсистемы." материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. ***Подготовка к практическим занятиям:*** Изучение материала по разделу "РАЗДЕЛ 2. Симметричные и асиммтетричные шифрсистемы." подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "РАЗДЕЛ 2. Симметричные и асиммтетричные шифрсистемы." ***Изучение материалов литературных источников:*** [1], 1-257 [2], 1-328 [3], 1-136
2.3	Тема 5. Концепция криптосистем с открытыми ключами и ее реализация на базе модулярной арифметики и эллиптических кривых.	16		2	2	4	-	-	-	-	-	8	-	

														[8], 116-180 [9], стр. 12-38
3	РАЗДЕЛ 3. Криптографические протоколы, хэш-функции и электронные подписи	34		4	4	10	-	-	-	-	-	16	-	***<u>Подготовка к текущему контролю:</u>*** Повторение материала по разделу "РАЗДЕЛ 3. Криптографические протоколы, хэш-функции и электронные подписи" ***<u>Подготовка к аудиторным занятиям:</u>***
3.1	Тема 6. Криптографические протоколы.	16		2	2	4	-	-	-	-	-	8	-	Проработка лекции, выполнение и подготовка к защите лаб. работы ***<u>Подготовка домашнего задания:</u>***
3.2	Тема 7. Хэш-функции и электронные подписи.	18		2	2	6	-	-	-	-	-	8	-	Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "РАЗДЕЛ 3. Криптографические протоколы, хэш-функции и электронные подписи" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. ***<u>Подготовка к контрольной работе:</u>*** Изучение материалов по разделу РАЗДЕЛ 3. Криптографические протоколы, хэш-функции и электронные подписи и подготовка к контрольной работе ***<u>Подготовка к практическим занятиям:</u>*** Изучение материала по разделу "РАЗДЕЛ 3. Криптографические протоколы, хэш-функции и электронные подписи" подготовка к выполнению заданий на практических занятиях ***<u>Самостоятельное изучение теоретического материала:</u>*** Изучение дополнительного материала по разделу "РАЗДЕЛ 3. Криптографические протоколы, хэш-функции и электронные подписи" ***<u>Изучение материалов литературных источников:</u>***

														[4], 1-512 [5], 1-200 [8], 253-285 [9], стр. 52-95
	Экзамен	36.0		-	-	-	-	2	-	-	0.5	-	33.5	
	Всего за семестр	**144.0**		**14**	**14**	**28**	-	**2**	-	-	**0.5**	**52**	**33.5**	
	Итого за семестр	**144.0**		**14**	**14**	**28**	**2**		**-**		**0.5**	**85.5**		

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. РАЗДЕЛ 1. Основы криптографической защиты информации.

1.1. Введение

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. Виды и формы отчетности. Рекомендуемые учебные пособия основной и дополнительной литературы по дисциплине..

1.2. Тема 1. Основные понятия криптографической защиты информации

Особенности задач криптографической защиты информации. Нормативная база в области 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

Классификация средств криптографической 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. РАЗДЕЛ 2. Симметричные и асимметричные шифрсистемы.

2.1. Тема 3. Симметричные блочные шифры.

Принципы построения блочных шифров. Американский стандарт шифрования данных DES. Отечественный стандарт шифрования данных ГОСТ 28147-89. 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.

Однонаправленные функции. Особенности использования асимметричных криптосистем. Шифрсистема RSA, возможные атаки на нее. Шифрсистема Эль-Гамаля. Кодирование и шифрование, шифрсистема Мак-Элиса. Шифрсистема на основе «проблемы рюкзака». Шифрсистема Полига-Хеллмана. Криптосистемы на эллиптических кривых..

3. РАЗДЕЛ 3. Криптографические протоколы, хэш-функции и электронные подписи

3.1. Тема 6. 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 7. 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. Методы вычисления коллизий для хэш-функций. 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. Схемы слепой и неоспоримой подписи. Стандарты на электронные подписи..

3.3. Темы практических занятий

1. Криптографические протоколы. Примеры протоколов идентификации и аутентификации пользователей и криптопротоколов на эллиптических кривых.;
2. Асимметричные шифрсистемы. Реализация расширенного алгоритма Евклида и его модификации в виде метода Гаусса. Реализация шифрсистемы RSA.;
3. Поточные шифры. Примеры реализации синхронных и асинхронных шифров.;
4. Симметричные блочные шифры. Реализация операций отечественного стандарта шифрования данных ГОСТ 28147-89.;
5. Симметричные блочные шифры. Стандарт шифрования данных AES. Реализация вычислений в конечных полях Галуа GF(28). Реализация операции BS. Обработка четырех-байтовых массивов (слов).;
6. 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. Методы вычисления коллизий для хэш-функций. 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. Схемы слепой и неоспоримой подписи. Стандарты на электронные подписи.;
7. Криптографические генераторы и их виды. Фильтрующие генераторы. Комбинирующие генераторы. Генераторы гаммы с неравномерным движением. Генераторы с дополнительной памятью.;
8. Линейная сложность последовательности и ее определение посредством использования алгоритма Берлекемпа-Месси.;
9. Псевдослучайные последовательности. Подходы к анализу этих последовательностей, требования к ним и тестирование. Линейные рекуррентные последовательности (ЛРП) и их реализация на линейных регистрах сдвига (ЛРС).;
10. Элементы криптоанализа шифров простой замены, шифров перестановки и шифров гаммирования.;
11. Хэш-функции. Реализация хэш-функций с помощью блочных шифров и специальных алгоритмов. Отечественный стандарт на хэш-функции.;
12. Симметричные блочные шифры. Стандарт шифрования данных DES. Реализация

пре-образований петли Фейстеля. Генерирование раундовых ключей.;
13. Электронные подписи. Примеры реализации алгоритмов электронной подписи RSA, Эль – Гамаля и DSA. Отечественный стандарт на электронную подпись..

3.4. Темы лабораторных работ

1. Лабораторная работа №5. Электронная подпись.;
2. Лабораторная работа №4. Стандарт симметричного шифрования AES.;
3. Лабораторная работа №3. Шифрование методом скользящей перестановки.;
4. Лабораторная работа №2. Исследование различных методов защиты текстовой информации и их стойкости на основе подбора ключей.;
5. Лабораторная работа № 1. Использование классических криптоалгоритмов подстановки и перестановки для защиты текстовой информации..

3.5 Консультации

Текущий контроль (ТК)

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "РАЗДЕЛ 1. Основы криптографической защиты информации."
2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "РАЗДЕЛ 2. Симметричные и асиммтетричные шифрсистемы."
3. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "РАЗДЕЛ 3. Криптографические протоколы, хэш-функции и электронные подписи"

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:					
действующую классификацию средств криптографической защиты информации	ПК-1(Компетенция)	+			Домашнее задание/Защита домашнего задания «Дешифрование классических шифров» Реферат/Защита реферата
состояние нормативно-законодательной базы и стандарты в области криптографической защиты информации	ПК-4(Компетенция)	+			Домашнее задание/Защита домашнего задания «Дешифрование классических шифров»
сущность системного подхода к защите информации	ПК-4(Компетенция)	+			Домашнее задание/Защита домашнего задания «Дешифрование классических шифров»
классификацию, требования к шифрам и основные характеристики шифров	ОК-5(Компетенция)	+			Домашнее задание/Защита домашнего задания «Дешифрование классических шифров»
принципы построения современных криптосистем и криптопротоколов	ПСК-2(Компетенция)		+		Реферат/Защита реферата Контрольная работа/Контрольная работа №1 «Симметричные и асимметричные криптосистемы»
Уметь:					
пользоваться стандартными математическими методами при анализе криптографических алгоритмов	ПК-1(Компетенция)	+			Реферат/Защита реферата
формулировать и решать задачи проектирования защищенных профессионально-ориентированных автоматизированных систем с использованием криптографических методов	ПК-4(Компетенция)		+		Контрольная работа/Контрольная работа №1 «Симметричные и асимметричные криптосистемы»

применять на практике положения законов РФ и ведомственных нормативных актов в области защиты информации	ОК-5(Компетенция)		+		Контрольная работа/Контрольная работа №1 «Симметричные и асимметричные криптосистемы»
применять криптографические методы защиты информации в различных предметных областях	ПСК-2(Компетенция)			+	Реферат/Защита реферата Контрольная работа/Контрольная работа №2. «Криптографические протоколы, хэш-функции и электронные подписи»

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

4.1. Текущий контроль успеваемости

6 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 №6)

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 6 семестр.

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

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Печатные и электронные издания:

1. Бабаш, А. В. Криптографические методы защиты информации : учебник по направлению "Прикладная информатика" / А. В. Бабаш, Е. К. Баранова . – М. : КноРус, 2016 . – 190 с. – (Бакалавриат и магистратура) . - ISBN 978-5-406-04766-8 .;
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. 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 .;
4. 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 .;
5. 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 .;
6. Рябко, Б. Я. Криптографические методы защиты информации : учебное пособие для вузов по специальностям "Многоканальные телекоммуникационные системы", "Радиосвязь,

радиовещание и телевидение","Защитные системы связи" / Б. Я. Рябко, А. Н. Фионов . – 2-е изд., стереотип . – М. : Горячая Линия-Телеком, 2014 . – 229 с. - ISBN 978-5-9912-0286-2 .;
7. Смарт, Н. Криптография : пер. с англ. / Н. Смарт . – М. : Техносфера, 2005 . – 528 с. – (Мир программирования) . - ISBN 5-948360-43-1 .;
8. 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 .;
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. Майнд Видеоконференции;
5. Visio.

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. **ЭБС "Консультант студента"** - http://www.studentlibrary.ru/
5. **Электронная библиотека МЭИ (ЭБ МЭИ)** - http://elib.mpei.ru/login.php
6. **Информационно-справочная система «Кодекс/Техэксперт»** - Http:\\proinfosoft.ru; http://docs.cntd.ru/
7. **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	А-317, Учебная аудитория	парта со скамьей, стол преподавателя, стул, доска меловая
Учебные аудитории для проведения лабораторных занятий	А-317, Учебная аудитория	парта со скамьей, стол преподавателя, стул, доска меловая
Учебные аудитории для проведения промежуточной	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
	А-322, Учебная	парта со скамьей, стол преподавателя,

аттестации	аудитория "А"	стул, доска меловая
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	А-322, Учебная аудитория "А"	парта со скамьей, стол преподавателя, стул, доска меловая
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

Криптографические методы защиты информации

(название дисциплины)

6 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	РАЗДЕЛ 1. Основы криптографической защиты информации.					
1.1	Введение		+			+
1.2	Тема 1. Основные понятия криптографической защиты информации		+			+
1.3	Тема 2. Основы криптографических методов защиты информации		+			+
2	РАЗДЕЛ 2. Симметричные и асиммтетричные шифрсистемы.					
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.			+		+
3	РАЗДЕЛ 3. Криптографические протоколы, хэш-функции и электронные подписи					
3.1	Тема 6. Криптографические протоколы.				+	+
3.2	Тема 7. Хэш-функции и электронные подписи.				+	+
		Вес КМ, %:	25	25	25	25