Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Национальный исследовательский университет «МЭИ»

Направление подготовки/специальность: 11.05.01 Радиоэлектронные системы и комплексы

Наименование образовательной программы: Радионавигационные системы и комплексы

Уровень образования: высшее образование - специалитет

Форма обучения: Очная

Рабочая программа дисциплины
ЗАЩИТА ИНФОРМАЦИИ В РАДИОЭЛЕКТРОННЫХ СИСТЕМАХ

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Часть, формируемая участниками образовательных отношений**
№ дисциплины по учебному плану:	**Б4.Ч.02**
Трудоемкость в зачетных единицах:	**9 семестр - 2;**
Часов (всего) по учебному плану:	**72 часа**
Лекции	**9 семестр - 16 часов;**
Практические занятия	**9 семестр - 16 часов;**
Лабораторные работы	**не предусмотрено учебным планом**
Консультации	**проводится в рамках часов аудиторных занятий**
Самостоятельная работа	**9 семестр - 39,7 часа;**
в том числе на КП/КР	**не предусмотрено учебным планом**
Иная контактная работа	**проводится в рамках часов аудиторных занятий**
включая: **Коллоквиум** **Решение задач**	
Промежуточная аттестация:	
Зачет	**9 семестр - 0,3 часа;**

Москва 2018

ПРОГРАММУ СОСТАВИЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Губонин Н.С. Идентификатор: Rd0607fd3-GuboninNS-9d6214d0	Н.С. Губонин
(должность)	(подпись)	(расшифровка подписи)

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Сизякова А.Ю. Идентификатор: R4eb30863-SiziakovaAY-83831ea7	А.Ю. Сизякова
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)
Заведующий выпускающей кафедры	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Куликов Р.С. Идентификатор: R7ef0b374-KulikovRS-e851162c	Р.С. Куликов
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины: состоит в изучении методов и способов защиты информационного содержания передаваемых сообщений для последующего использования при создании, модернизации и эксплуатации радиоэлектронной аппаратуры разного уровня (систем, комплексов, устройств)

Задачи дисциплины

- изучение общих понятий информационной безопасности (ИБ) радиоэлектронных систем и общих подходов к её обеспечению;
- изучение криптографических методов защиты информации при её хранении и передаче;
- изучение современных средств технической реализации защиты информации при хранении и передаче по проводным линиям цифровой связи и радиоканалам;
- изучение особенностей защиты информации в информационных (компьютерных) сетях.

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 структурные и функциональные схемы подсистем радиоэлектронных систем и комплексов, в том числе с использованием математического моделирования алгоритмов формирования, передачи, приема и обработки радиосигналов	ИД-1$_{ПК-1}$ Знает методы выполнения расчетов основных технических характеристик схем подсистем радиоэлектронных систем и комплексов	знать: - математический аппарат, используемый в алгоритмах шифрования и расшифровывания данных, принципы защиты информации; - современные криптографические методы обеспечения информационной безопасности локальных и распределённых радиоэлектронных систем обработки информации; - основные угрозы безопасности РЭС и пути их предотвращения.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к факультативным дисциплинам основной профессиональной образовательной программе Радионавигационные системы и комплексы (далее – ОПОП), направления подготовки 11.05.01 Радиоэлектронные системы и комплексы, уровень образования: высшее образование - специалитет.

Требования к входным знаниям и умениям:

- знать назначение и общие принципы работы различных радиотехнических систем и их блоков, а также используемую при их реализации элементную базу
- знать терминологию и возможности основных инструментальных средств локальных информационных технологий
- знать высшую математику
- знать основы построения и разновидности радиотехнических систем
- уметь проводить сопоставительный анализ вариантов технических решений, используя показатели сравнения в шкале наименований (лингвистической шкале)
- уметь использовать графические модели (схемы, рисунки, графики, графы) для иллюстрации взаимосвязей в изучаемых объектах

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 2 зачетных единицы, 72 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	Принципы защиты информации в автоматизированных системах обработки информации	11.7	9	2	-	2	-	-	-	-	-	7.7	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "1.Принципы защиты информации в автоматизированных системах обработки информации."
1.1	Принципы защиты информации в автоматизированных системах обработки информации	11.7		2	-	2	-	-	-	-	-	7.7	-	***Подготовка расчетных заданий:*** Выполнение 1-ой части комплексного расчётного задания (КРЗ) Комплексное расчётное задание состоит из 2-х частей и выполняется индивидуально по вариантам. Первая часть предполагает развёрнутый мотивированный ответ объёмом 3-10с на общий вопрос по организации защиты информации в РЭС разных классов. Вторая часть содержит набор из 6-и задач на методы симметричного и асимметричного шифрования. Примеры тем 1-ой части КРЗ: - Дайте развёрнутый ответ (объёмом 3-10с машинописного текста на вопрос: «Какие основные методы организации защиты данных используются в современных беспроводных (радио) многоканальных телекоммуникационных системах и вызовы, которые приходится при этом преодолевать, в связи с бурным развитием информационных технологий?» - Дайте развёрнутый ответ (объёмом 3-10с машинописного текста на вопрос: «Какие

														основные методы организации защиты данных используются в современных кабельных многоканальных телекоммуникационных системах и вызовы, которые приходится при этом преодолевать, в связи с бурным развитием информационных технологий?» - Дайте развёрнутый ответ (объёмом 3-10с машинописного текста на вопрос: «Какие основные методы организации защиты данных используются в современных спутниковых многоканальных телекоммуникационных системах фиксированной связи и вызовы, которые приходится при этом преодолевать, в связи с бурным развитием информационных технологий?» - Дайте развёрнутый ответ (объёмом 3-10с машинописного текста на вопрос: «Какие основные методы организации защиты данных используются в современных оптоволоконных многоканальных телекоммуникационных системах и вызовы, которые приходится при этом преодолевать, в связи с бурным развитием информационных технологий?» ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Принципы защиты информации в автоматизированных системах обработки информации." Подготовка к выполнению заданий на практических (семинарских) занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Принципы защиты информации в автоматизированных системах обработки информации" ***Изучение материалов литературных источников:*** [2], стр. 4-12

														[3], стр. 43-50
2	Элементы дискретной математики (алгебра и теория чисел)	16		4	-	4	-	-	-	-	-	8	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Элементы дискретной математики (алгебра и теория чисел)" ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Элементы дискретной математики (алгебра и теория чисел)" Подготовка к выполнению заданий на практических (семинарских) занятиях ***Подготовка расчетных заданий:*** Задания ориентированы на решения минизадач по разделу "Элементы дискретной математики (алгебра и теория чисел)". Студенту необходимо повторить теоретический материал, разобрать примеры решения аналогичных задач. провести расчеты по варианту задания и сделать выводы ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Элементы дискретной математики (алгебра и теория чисел)" ***Изучение материалов литературных источников:*** [2], стр. 52-72
2.1	Элементы дискретной математики (алгебра и теория чисел)	16		4	-	4	-	-	-	-	-	8	-	
3	Симметричные системы шифрования	22		6	-	6	-	-	-	-	-	10	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Симметричные системы шифрования" ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Симметричные системы шифрования" Подготовка к выполнению заданий на практических (семинарских) занятиях ***Подготовка расчетных заданий:*** Задания ориентированы на решения минизадач по разделу "Симметричные системы шифрования". Студенты необходимо повторить теоретический материал,
3.1	Симметричные системы шифрования	22		6	-	6	-	-	-	-	-	10	-	

														разобрать примеры решения аналогичных задач. провести расчеты по варианту задания и сделать выводы. В качестве задания используются следующие упражнения: Задача 1.Зашифруйте слово КРИПТОЗАЩИТА, используя в качестве ключа таблицу 2x6, перестановку строк по ключевому слову ДА и перестановку столбцов по ключевому слову АЗИМУТ. Ответ поясните. Задача 2 Зашифруйте слово ИНФОРМАЦИЯ методом аффинной подстановки с параметрами a=4, k=2 , используя алфавит русских прописных букв {А, Б, В...Я}, который эквивалентен цифровому алфавиту {0, 1, 2,...,32}. Ответ поясните. Задача 3 Зашифруйте слово ИНФОРМАЦИЯ методом подстановки по ключевому слову СОН в алфавите, состоящем из русских прописных букв {А, Б, В...Я}, который эквивалентен цифровому алфавиту {0, 1, 2,..., 32}. Ответ поясните. Задача 4 Можно ли при шифровании методом Хилла сообщения на русском языке в алфавите из 33 прописных букв и символа пробела применить линейное преобразование с матрицей T (задаётся конкретная целочисленная матрица размера 3x3)? Ответ поясните. Задача 5 Сколько в среднем придётся провести последовательных испытаний для определения ключа сообщения на русском языке (объём алфавита n=34), зашифрованного в системе шифрования Цезаря? ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Симметричные системы шифрования" ***Изучение материалов литературных источников:***

														[3], стр. 294-321 [4], стр. 185-208
4	Системы шифрования с открытым ключом (асимметричные системы шифрования)	14		2	-	2	-	-	-	-	-	10	-	***Подготовка расчетных заданий:*** Задания ориентированы на решения минизадач по разделу "Системы шифрования с открытым ключом (асимметричные системы шифрования)". Студенты необходимо повторить теоретический материал, разобрать примеры решения аналогичных задач. провести расчеты по варианту задания и сделать выводы. В качестве задания используются следующие упражнения: Задача 1 Зашифруйте методом RSA с открытым ключом (n. k)=(33, 7) в алфавите , состоящем из русских прописных букв {А, Б, В...Я}, который эквивалентен цифровому алфавиту {0, 1, 2,..., 32}, слово НАДЕЖДА. Ответ поясните. ***Подготовка к текущему контролю:*** Повторение материала по разделу "Системы шифрования с открытым ключом (асимметричные системы шифрования)" ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Системы шифрования с открытым ключом (асимметричные системы шифрования)" Подготовка к выполнению заданий на практических (семинарских) занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Системы шифрования с открытым ключом (асимметричные системы шифрования)" ***Изучение материалов литературных источников:*** [1], стр. 14-65
4.1	Системы шифрования с открытым ключом (асимметричные системы шифрования)	14		2	-	2	-	-	-	-	-	10	-	
5	Защита данных в информационных сетях	8		2	-	2	-	-	-	-	-	4	-	

5.1	Защита данных в информационных сетях	8		2	-	2	-	-	-	-	-	4	-	
	Зачет	0.3		-	-	-	-	-	-	-	0.3	-	-	
	Всего за семестр	**72.0**		**16**	**-**	**16**	**-**	**-**	**-**	**-**	**0.3**	**39.7**	**-**	
	Итого за семестр	**72.0**		**16**	**-**	**16**	**-**		**-**		**0.3**	**39.7**		

Примечание: Лек – лекции; Лаб – лабораторные работы; Пр – практические занятия; КПР – аудиторные консультации по курсовым проектам/работам; ИККП – индивидуальные консультации по курсовым проектам/работам; ГК- групповые консультации по разделам дисциплины; СР – самостоятельная работа студента; ИКР – иная контактная работа; ТК – текущий контроль; ПА – промежуточная аттестация

3.2 Краткое содержание разделов

1. Принципы защиты информации в автоматизированных системах обработки информации

1.1. Принципы защиты информации в автоматизированных системах обработки информации

Общая характеристика проблемы защиты информации при её хранении, передаче, извлечении и обработке электронными средствами. Основные понятия и определения информационной безопасности. Угрозы и обеспечение безопасности в автоматизированных системах обработки информации. Общая характеристика принципов криптологии и средств защиты информации. Принципы криптографической защиты информации. Принципы криптоанализа. Виды и классификация средств защиты информации.

2. Элементы дискретной математики (алгебра и теория чисел)

2.1. Элементы дискретной математики (алгебра и теория чисел)

Алгебраические операции по mod n . Наибольший общий делитель и алгоритмы его отыскания. Определения и примеры. Алгоритм Евклида. Расширенный алгоритма Евклида. Вычисление обратных величин по mod n. Функция Эйлера для числа элементов приведённого набора вычетов. Определение. Функция Эйлера для числа элементов приведённого набора вычетов. Вычисление обратных величин по mod n методом перебора, с применением функции Эйлера, с использованием расширенного алгоритма Эвклида вычисления НОД. Примеры. Группы, кольца, поля. Конечные поля. Поля Галуа. Линейные пространства над конечным кольцом. Определения, свойства и примеры. Функции со специальными свойствами. Однонаправленные функции. Хэш-функции. Определения, свойства и примеры. Построение Хэш функций.

3. Симметричные системы шифрования

3.1. Симметричные системы шифрования

Шифрование методом перестановок. Определение. Шифрование с использованием размеров таблицы в качестве ключа. Шифрование с дополнительной перестановкой столбцов или (и) строк. Шифрование методом замены (подстановок). Определение. Система шифрования Цезаря. Система аффинных подстановок Цезаря. Криптографическая система Хилла. Шифрование методом многоалфавитных подстановок и методом гаммирования. Метод простой (одноконтурной) многоалфавитной подстановки. Метод g-контурной многоалфавитной подстановки. Понятие о системе шифрования Вермена. Метод гаммирования. Стандарт шифрования данных DES. Общее описание алгоритмов шифрования и расшифрования DES Использование алгоритма DES. Комбинирование блочных алгоритмов. Основные режимы алгоритма DES. Области применения алгоритма DES. Комбинирование блочных алгоритмов. Российский стандарт шифрования. Алгоритмы шифрования и расшифрования в режиме простой замены. Режим гаммирования. Режим гаммирования с обратной связью. Формирование имитовставки. Общая характеристика стандарта шифрования данных AES. Математическая теория и алгоритм шифрования данных. Математическая теория процедур расширения ключа и расшифрования. Алгоритм расширения ключа, алгоритм расшифрования и эквивалентный алгоритм расшифрования данных.

4. Системы шифрования с открытым ключом (асимметричные системы шифрования)

4.1. Системы шифрования с открытым ключом (асимметричные системы шифрования)

Система шифрования RSA. Принцип построения систем шифрования с открытым ключом. Протоколы и алгоритмы шифрования и расшифрования в системе RSA. Системы шифрования, использующие задачу дискретного логарифмирования. Задача дискретного логарифмирования. Протоколы и алгоритмы шифрования и расшифрования в системе Эль-Гамаля. Использование группы точек эллиптической кривой. Криптографические протоколы в системе ECIES.

5. Защита данных в информационных сетях

5.1. Защита данных в информационных сетях

Слабая идентификация (фиксированные пароли). Типовые схемы..Сильная идентификация (системы «запрос-ответ»).Использование симметричных и асимметричных . алгоритмов шифрования. Электронная цифровая подпись. Определение, методы реализации и возможные алгоритмы электронной цифровой подписи. Удалённые атаки в сети Internet. Виды и классификация моделей типовых сетевых атак. Основные методы и средства сетевой защиты.

3.3. Темы практических занятий

1. Удалённые атаки в сети Internet: виды и классификация. Основные методы и средства сетевой защиты;
2. Системы шифрования, использующие задачу дискретного логарифмирования при шифровании. Протоколы и алгоритмы в системе Эль-Гамаля. Использование группы точек эллиптической кривой. Криптографические протоколы в системе ECIES;
3. Общая характеристика стандарта шифрования данных AES. Математическая теория и алгоритм шифрования данных. Математическая теория процедур расширения ключа и расшифрования. Алгоритм расширения ключа, алгоритм расшифрования и эквивалентный алгоритм расшифрования данных;
4. Стандарт шифрования DES. Общее описание алгоритмов шифрования и расшифрования DES Использование алгоритма DES. Комбинирование блочных алгоритмов. Основные режимы алгоритма DES. Области применения алгоритма DES. Комбинирование блочных алгоритмов;
5. Шифрование методом замены (методом подстановок). Система шифрования Цезаря и система аффинных подстановок Цезаря. Криптографическая система Хилла;
6. Функции со специальными свойствами. Однонаправленные функции. Хэш-функции. Определения, свойства и примеры;
7. Вычисление обратных величин по mod n. Функция Эйлера для приведённого набора вычетов;
8. Общая характеристика принципов криптологии и аппаратно-программные средства защиты информации. Принципы криптографической защиты информации. Принципы криптоанализа.

3.4. Темы лабораторных работ

не предусмотрено

3.5 Консультации

Текущий контроль (ТК)

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Принципы защиты информации в автоматизированных системах обработки информации"

2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Элементы дискретной математики (алгебра и теория чисел)"
3. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Симметричные системы шифрования"
4. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Системы шифрования с открытым ключом (асимметричные системы шифрования)"
5. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Защита данных в информационных сетях"

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	
Знать:							
основные угрозы безопасности РЭС и пути их предотвращения	ИД-1$_{ПК-1}$			+			Коллоквиум/Коллоквиум №3. Криптографические функции со специальными свойствами. Опасные воздействия на РЭС Коллоквиум/Коллоквиум №4 Шифрование с использованием шифровальной таблицы. Реализация угроз безопасности РЭС Коллоквиум/Коллоквиум №5 Шифрование методом Хилла. Меры обеспечения безопасности компьютерных систем Коллоквиум/Коллоквиум № 6 Российский стандарт шифрования, стандарты DES и AES
современные криптографические методы обеспечения информационной безопасности локальных и распределённых радиоэлектронных систем обработки информации	ИД-1$_{ПК-1}$				+	+	Коллоквиум/Коллоквиум № 7 Система шифрования с открытым ключом RSA. Идентификация и аутентификация электронных данных Коллоквиум/Коллоквиум № 8 Сильная и слабая идентификация. Принципы проектирования систем защиты информации Решение задач/Комплексное расчетное задание
математический аппарат, используемый в алгоритмах шифрования и расшифровывания данных, принципы защиты информации	ИД-1$_{ПК-1}$	+	+				Коллоквиум/Коллоквиум №1. Основные понятия защиты информации Коллоквиум/Коллоквиум №2. Модулярные операции. Угрозы безопасности РЭС

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

4.1. Текущий контроль успеваемости

9 семестр

Форма реализации: Письменная работа

1. Коллоквиум № 6 Российский стандарт шифрования, стандарты DES и AES (Коллоквиум)
2. Коллоквиум № 7 Система шифрования с открытым ключом RSA. Идентификация и аутентификация электронных данных (Коллоквиум)
3. Коллоквиум № 8 Сильная и слабая идентификация. Принципы проектирования систем защиты информации (Коллоквиум)
4. Коллоквиум №1. Основные понятия защиты информации (Коллоквиум)
5. Коллоквиум №2. Модулярные операции. Угрозы безопасности РЭС (Коллоквиум)
6. Коллоквиум №3. Криптографические функции со специальными свойствами. Опасные воздействия на РЭС (Коллоквиум)
7. Коллоквиум №4 Шифрование с использованием шифровальной таблицы. Реализация угроз безопасности РЭС (Коллоквиум)
8. Коллоквиум №5 Шифрование методом Хилла. Меры обеспечения безопасности компьютерных систем (Коллоквиум)

Форма реализации: Проверка задания

1. Комплексное расчетное задание (Решение задач)

Балльно-рейтинговая структура дисциплины является приложением А.

4.2 Промежуточная аттестация по дисциплине

Зачет (Семестр №9)

Оценка за освоение дисциплины определяется как семестровая оценка в соответствии с «Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ»

В диплом выставляется оценка за 9 семестр.

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

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Печатные и электронные издания:

1. Губонин, Н. С. Ассиметричные криптосистемы и борьба с сетевыми угрозами : учебное пособие по курсу "Защита информации в системах передачи и обработки данных" по направлениям "Радиотехника", "Радиоэлектронные системы и комплексы" / Н. С. Губонин, Нац. исслед. ун-т "МЭИ" . – М. : Изд-во МЭИ, 2015 . – 84 с. - ISBN 978-5-7046-1666-5 . http://elib.mpei.ru/action.php?kt_path_info=ktcore.SecViewPlugin.actions.document&fDocumentId=7494;
2. Губонин, Н. С. Защита информации в системах передачи и обработки данных. Часть 1 : учебное пособие по курсу "Защита информации в системах передачи и обработки данных" по направлению "Радиотехника" / Н. С. Губонин, Нац. исслед. ун-т "МЭИ" . – М. : Изд-во МЭИ, 2013 . – 88 с. - ISBN 978-5-9902974-2-5 .

http://elib.mpei.ru/action.php?kt_path_info=ktcore.SecViewPlugin.actions.document&fDocumentId=5673;
3. Шаньгин В. Ф.- "Защита информации в компьютерных системах и сетях", Издательство: "ДМК Пресс", Москва, 2012 - (592 с.)
http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=3032;
4. 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. Майнд Видеоконференции;
5. Acrobat Reader.

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 ВИНИТИ online** - http://www.viniti.ru/
5. **Национальная электронная библиотека** - https://rusneb.ru/
6. **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	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
	Ж-400/5, Лаборатория «Системы передачи информации»	стол преподавателя, стол, стул, шкаф для документов, доска меловая, компьютерная сеть с выходом в Интернет, указка, стенд лабораторный
Учебные аудитории для проведения практических занятий, КР и КП	Ж-400/5, Лаборатория «Системы передачи информации»	стол преподавателя, стол, стул, шкаф для документов, доска меловая, компьютерная сеть с выходом в Интернет, указка, стенд лабораторный
Учебные аудитории для проведения промежуточной аттестации	Ж-400/5, Лаборатория «Системы передачи информации»	стол преподавателя, стол, стул, шкаф для документов, доска меловая, компьютерная сеть с выходом в Интернет, указка, стенд лабораторный
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	Ж-400/3, Консультационный зал каф. "РТС"	стол, стул, шкаф для документов, книги, учебники, пособия
Помещения для хранения оборудования и учебного инвентаря	Ж-400/9, Прочее каф. "РТС"	стеллаж для хранения книг, стул, книги, учебники, пособия

Приложение А

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Защита информации в радиоэлектронных системах

(название дисциплины)

9 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

КМ-1 Коллоквиум №1. Основные понятия защиты информации (Коллоквиум)
КМ-2 Коллоквиум №2. Модулярные операции. Угрозы безопасности РЭС (Коллоквиум)
КМ-3 Коллоквиум №3. Криптографические функции со специальными свойствами. Опасные воздействия на РЭС (Коллоквиум)
КМ-4 Коллоквиум №4 Шифрование с использованием шифровальной таблицы. Реализация угроз безопасности РЭС (Коллоквиум)
КМ-5 Коллоквиум №5 Шифрование методом Хилла. Меры обеспечения безопасности компьютерных систем (Коллоквиум)
КМ-6 Коллоквиум № 6 Российский стандарт шифрования, стандарты DES и AES (Коллоквиум)
КМ-7 Коллоквиум № 7 Система шифрования с открытым ключом RSA. Идентификация и аутентификация электронных данных (Коллоквиум)
КМ-8 Коллоквиум № 8 Сильная и слабая идентификация. Принципы проектирования систем защиты информации (Коллоквиум)
КМ-9 Комплексное расчетное задание (Решение задач)

Вид промежуточной аттестации – Зачет.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4	КМ-5	КМ-6	КМ-7	КМ-8	КМ-9
		Неделя КМ:	4	6	8	10	12	14	15	15	16
1	Принципы защиты информации в автоматизированных системах обработки информации										
1.1	Принципы защиты информации в автоматизированных системах обработки информации		+	+							
2	Элементы дискретной математики (алгебра и теория чисел)										
2.1	Элементы дискретной математики (алгебра и теория чисел)		+	+							
3	Симметричные системы шифрования										
3.1	Симметричные системы шифрования				+	+	+	+			

4	Системы шифрования с открытым ключом (асимметричные системы шифрования)									
4.1	Системы шифрования с открытым ключом (асимметричные системы шифрования)							+	+	+
5	Защита данных в информационных сетях									
5.1	Защита данных в информационных сетях							+	+	+
	Вес КМ, %:	8	8	8	8	8	8	8	8	36