Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Национальный исследовательский университет «МЭИ»

Направление подготовки/специальность: 11.04.01 Радиотехника

Наименование образовательной программы: Радиотехнические системы

Уровень образования: высшее образование - магистратура

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:	**Б1.Ч.06.01.02**
Трудоемкость в зачетных единицах:	**1 семестр - 3;**
Часов (всего) по учебному плану:	**108 часов**
Лекции	**1 семестр - 16 часов;**
Практические занятия	**1 семестр - 16 часов;**
Лабораторные работы	**не предусмотрено учебным планом**
Консультации	**проводится в рамках часов аудиторных занятий**
Самостоятельная работа	**1 семестр - 75,7 часа;**
в том числе на КП/КР	**не предусмотрено учебным планом**
Иная контактная работа	**проводится в рамках часов аудиторных занятий**
включая: **Проверочная работа**	
Промежуточная аттестация:	
Зачет с оценкой	**1 семестр - 0,3 часа;**

Москва 2024

ПРОГРАММУ СОСТАВИЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Бровко Т.А. Идентификатор: R2d31a545-BrovkoTA-c057cc38	Т.А. Бровко

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Комаров А.А. Идентификатор: R8495daf1-KomarovAlA-eada3f0e	А.А. Комаров
Заведующий выпускающей кафедрой	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Комаров А.А. Идентификатор: R8495daf1-KomarovAlA-eada3f0e	А.А. Комаров

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 передач;
- 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 проводить исследования в целях совершенствования радиоэлектронных систем	ИД-З$_{ПК-1}$ Разрабатывает алгоритмы и проводит исследования в целях совершенствования функциональных узлов радиоэлектронных систем	знать: - современные криптографические методы обеспечения информационной безопасности локальных и распределённых радиоэлектронных систем обработки информации; - основные угрозы безопасности РЭС и пути их предотвращения; - общие понятия и принципы защиты информации в информационных радиоэлектронных системах (РЭС); - математический аппарат, используемый в алгоритмах шифрования и расшифровывания данных, принципы защиты информации. уметь: - проводить сопоставительный анализ и рациональный выбор по совокупности показателей качества из существующих и перспективных методов и систем шифрования и расшифрования данных.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к основной профессиональной образовательной программе Радиотехнические системы (далее – ОПОП), направления подготовки 11.04.01 Радиотехника, уровень образования: высшее образование - магистратура.

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 для освоения дисциплины необходимо знать высшую математику
- знать для освоения дисциплины необходимо 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 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	Принципы защиты информации в автоматизированных системах обработки информации	21	1	4	-	2	-	-	-	-	-	15	-	***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "1.Принципы защиты информации в автоматизированных системах обработки информации" ***Подготовка к текущему контролю:*** Повторение материала по разделу "1.Принципы защиты информации в автоматизированных системах обработки информации." ***Подготовка к практическим занятиям:*** Изучение материала по разделу "1.Принципы защиты информации в автоматизированных системах обработки информации." Подготовка к выполнению заданий на практических (семинарских) занятиях ***Изучение материалов литературных источников:*** [3], стр. 10-19
1.1	Принципы защиты информации в автоматизированных системах обработки информации	21		4	-	2	-	-	-	-	-	15	-	
2	Элементы дискретной математики (алгебра и теория чисел)	21		4	-	2	-	-	-	-	-	15	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Элементы дискретной математики (алгебра и теория чисел)" ***Подготовка к аудиторным занятиям:*** Проработка материалов лекций и семинарских (практических) занятий
2.1	Элементы дискретной математики (алгебра и теория чисел)	21		4	-	2	-	-	-	-	-	15	-	

														Самостоятельное изучение теоретического материала: Изучение дополнительного 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 ***Изучение материалов литературных источников:*** [1], стр. 34-42
3	Симметричные системы шифрования	25		4	-	6	-	-	-	-	-	15	-	***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Симметричные системы шифрования" ***Подготовка к аудиторным занятиям:*** Проработка материалов лекций и семинарских (практических) занятий ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Симметричные системы шифрования" Подготовка к выполнению заданий на практических (семинарских) занятиях ***Подготовка к текущему контролю:*** Повторение материала по разделу "Симметричные системы шифрования" ***Изучение материалов литературных источников:*** [2], стр. 5-16
3.1	Симметричные системы шифрования	25		4	-	6	-	-	-	-	-	15	-	
4	Системы шифрования с открытым ключом (асимметричные системы шифрования). Защита данных в информационных сетях	40.7		4	-	6	-	-	-	-	-	30.7	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Системы шифрования с открытым ключом (асимметричные системы шифрования)" ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Системы шифрования с открытым ключом

4.1	Системы шифрования с открытым ключом (асимметричные системы шифрования). Защита данных в информационных сетях	40.7		4	-	6	-	-	-	-	-	30.7	-	(асимметричные системы шифрования)". Защита данных в информационных сетях. ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Системы шифрования с открытым ключом (асимметричные системы шифрования)". Защита данных в информационных сетях. Подготовка к выполнению заданий на практических (семинарских) занятиях ***Подготовка к аудиторным занятиям:*** Проработка материалов лекций и семинарских (практических) занятий ***Изучение материалов литературных источников:*** [2], стр.19-28 [4], стр. 25-51
	Зачет с оценкой	0.3		-	-	-	-	-	-	-	0.3	-	-	
	Всего за семестр	**108.0**		**16**	**-**	**16**	**-**	**-**	**-**	**-**	**0.3**	**75.7**	**-**	
	Итого за семестр	**108.0**		**16**	**-**	**16**	**-**		**-**		**0.3**	**75.7**		

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)

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. Шифрование с использованием размеров таблицы в качестве ключа, с дополнительной перестановкой столбцов или (и) строк, методом замены (подстановок). Система шифрования Цезаря. Криптографическая система Хилла. Метод простой (одноконтурной) многоалфавитной подстановки. Понятие о системе шифрования Вермена. Метод гаммирования. Стандарт шифрования данных 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). Защита данных в информационных сетях

4.1. Системы шифрования с открытым ключом (асимметричные системы шифрования). Защита данных в информационных сетях

Система шифрования 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. Слабая идентификация (фиксированные пароли). Сильная идентификация (системы «запрос-ответ»). Электронная цифровая подпись. Удалённые атаки в сети Internet. Виды и классификация моделей типовых сетевых атак. Основные методы и средства сетевой защиты.

3.3. Темы практических занятий

1. Общая характеристика принципов криптологии и аппаратно-программные средства защиты информации. Принципы криптографической защиты информации. Принципы криптоанализа;
2. Вычисление обратных величин по mod n. Функция Эйлера для приведённого набора вычетов;
3. Функции со специальными свойствами. Однонаправленные функции. Хэш-функции. Определения, свойства и примеры;
4. Шифрование методом замены (методом подстановок). Система шифрования Цезаря и система аффинных подстановок Цезаря. Криптографическая система Хилла;
5. 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;
6. 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;
7. 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;
8. Удалённые атаки в сети Internet: виды и классификация. Основные методы и средства сетевой защиты.

3.4. Темы лабораторных работ

не предусмотрено

3.5 Консультации

Групповые консультации по разделам дисциплины (ГК)

1. Консультации направлены на подготовку к контрольным мероприятиям по разделу "Принципы защиты информации в автоматизированных системах обработки информации"
2. Консультации направлены на подготовку к контрольным мероприятиям по разделу "Элементы дискретной математики (алгебра и теория чисел)"
3. Консультации направлены на подготовку к контрольным мероприятиям по разделу "Симметричные системы шифрования"
4. Консультации направлены на подготовку к контрольным мероприятиям по разделу "Системы шифрования с открытым ключом (асимметричные системы шифрования)"

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	
Знать:						
математический аппарат, используемый в алгоритмах шифрования и расшифровывания данных, принципы защиты информации	ИД-З$_{ПК-1}$		+			Проверочная работа/Линейные пространства над конечным кольцом
общие понятия и принципы защиты информации в информационных радиоэлектронных системах (РЭС)	ИД-З$_{ПК-1}$	+				Проверочная работа/Основные понятия защиты информации
основные угрозы безопасности РЭС и пути их предотвращения	ИД-З$_{ПК-1}$				+	Проверочная работа/Асимметричные системы шифрования
современные криптографические методы обеспечения информационной безопасности локальных и распределённых радиоэлектронных систем обработки информации	ИД-З$_{ПК-1}$	+				Проверочная работа/Основные понятия защиты информации
Уметь:						
проводить сопоставительный анализ и рациональный выбор по совокупности показателей качества из существующих и перспективных методов и систем шифрования и расшифрования данных	ИД-З$_{ПК-1}$			+		Проверочная работа/Симметричные системы шифрования

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

4.1. Текущий контроль успеваемости

1 семестр

Форма реализации: Смешанная форма

1. Асимметричные системы шифрования (Проверочная работа)
2. Линейные пространства над конечным кольцом (Проверочная работа)
3. Основные понятия защиты информации (Проверочная работа)
4. Симметричные системы шифрования (Проверочная работа)

Балльно-рейтинговая структура дисциплины является приложением А.

4.2 Промежуточная аттестация по дисциплине

Зачет с оценкой (Семестр №1)

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 1 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. 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/elib/view.php?id=5673;
2. 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/elib/view.php?id=7494;
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. Видеоконференции (Майнд, Сберджаз, ВК и др);

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. **Национальная электронная библиотека** - https://rusneb.ru/
5. **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-400д/10а, Учебная аудитория	парта со скамьей, стол преподавателя, стул, шкаф для одежды, доска меловая, кондиционер
	А-402, Учебная аудитория	парта, стул, доска меловая, колонки звуковые, мультимедийный проектор, доска маркерная, компьютер персональный, кондиционер
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-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	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)

1 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

КМ-1 Основные понятия защиты информации (Проверочная работа)
КМ-2 Линейные пространства над конечным кольцом (Проверочная работа)
КМ-3 Симметричные системы шифрования (Проверочная работа)
КМ-4 Асимметричные системы шифрования (Проверочная работа)

Вид промежуточной аттестации – Зачет с оценкой.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
		Неделя КМ:	4	8	12	15
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). Защита данных в информационных сетях					
4.1	Системы шифрования с открытым ключом (асимметричные системы шифрования). Защита данных в информационных сетях					+
		Вес КМ, %:	25	25	25	25