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 автоматизированных систем

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очно-заочная

Рабочая программа дисциплины
ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ КРИПТОГРАФИИ

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Вариативная**
№ дисциплины по учебному плану:	**Б1.В.07.03.02**
Трудоемкость в зачетных единицах:	**6 семестр - 6;**
Часов (всего) по учебному плану:	**216 часов**
Лекции	**6 семестр - 16 часов;**
Практические занятия	**6 семестр - 16 часов;**
Лабораторные работы	**не предусмотрено учебным планом**
Консультации	**проводится в рамках часов аудиторных занятий**
Самостоятельная работа	**6 семестр - 183,7 часа;**
в том числе на КП/КР	**не предусмотрено учебным планом**
Иная контактная работа	**проводится в рамках часов аудиторных занятий**
включая: **Контрольная работа**	
Промежуточная аттестация:	
Зачет с оценкой	**6 семестр - 0,3 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: Изучение математических методов, относящихся к теории чисел, применяемых при синтезе и анализе современных криптографических систем

Задачи дисциплины

- освоение терминологии и теоретико-числовых основ математики;;
- изучение современных достижений в теоретико-числовой области математики, используемым в области защиты информации;;
- приобретение навыков применения теоретико-числовых методов для решения задач обеспечения информационной безопасности;
- приобретение навыков постановки задач и поиска путей их решения.

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-2 способностью применять соответствующий математический аппарат для решения профессиональных задач		знать: - достижения в теоретико-числовой области математики, используемые при решении задач защиты информации. уметь: - определять требования к параметрам криптографических систем защиты информации.
ПК-10 способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности		знать: - алгоритмы факторизации целых чисел и дискретного логарифмирования. уметь: - применять теоретико-числовые методы для оценки стойкости криптографических систем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к части, формируемой участниками образовательных отношений блока дисциплин основной профессиональной образовательной программе Безопасность автоматизированных 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 6 зачетных единиц, 216 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	Теоретико - числовые основы	81	6	5	-	4	-	-	-	-	-	72	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Теоретико-числовые основы " ***Подготовка к аудиторным занятиям:*** Проработка лекции, изучение литературы ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Теоретико-числовые основы" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Теоретико-числовые основы " ***Изучение материалов литературных источников:*** [2], Гл. 2 [3], Гл. 1 [4], Гл.9 [5], Ч. 1
1.1	Введение	13		1	-	-	-	-	-	-	-	12	-	
1.2	Основы модулярной арифметики	34		2	-	2	-	-	-	-	-	30	-	
1.3	Эллиптические кривые	34		2	-	2	-	-	-	-	-	30	-	
2	Теоретико-числовые методы	80		8	-	8	-	-	-	-	-	64	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Теоретико-числовые методы" ***Подготовка к аудиторным занятиям:*** Проработка лекции, изучение литературы ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Теоретико-числовые методы " подготовка к выполнению заданий на практических
2.1	Простые числа и факторизация целых чисел	40		4	-	4	-	-	-	-	-	32	-	
2.2	Дискретное логарифмирование	40		4	-	4	-	-	-	-	-	32	-	

														занятиях ***<u>Самостоятельное изучение теоретического материала:</u>*** Изучение дополнительного материала по разделу "Теоретико-числовые методы " ***<u>Изучение материалов литературных источников:</u>*** [1], Гл. 1, 5, 6 [4], Гл. 13
3	Применение теоретико-числовых методов в криптографии	37		3	-	4	-	-	-	-	-	30	-	***<u>Подготовка к текущему контролю:</u>*** Повторение материала по разделу "Применение теоретико-числовых методов в криптографии"
3.1	Асимметричные криптосистемы	37		3	-	4	-	-	-	-	-	30	-	***<u>Подготовка к аудиторным занятиям:</u>*** Проработка лекции, изучение литературы ***<u>Подготовка к практическим занятиям:</u>*** Изучение материала по разделу "Применение теоретико-числовых методов в криптографии" подготовка к выполнению заданий на практических занятиях ***<u>Самостоятельное изучение теоретического материала:</u>*** Изучение дополнительного материала по разделу "Применение теоретико-числовых методов в криптографии" ***<u>Изучение материалов литературных источников:</u>*** [4], !л. 10,11, 14 [5], Гл. 11
	Зачет с оценкой	18.0		-	-	-	-	-	-	-	0.3	-	17.7	
	Всего за семестр	**216.0**		**16**	**-**	**16**	**-**	**-**	**-**	**-**	**0.3**	**166**	**17.7**	
	Итого за семестр	**216.0**		**16**	**-**	**16**	**-**		**-**		**0.3**	**183.7**		

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. Теоретико - числовые основы

1.1. Введение

Предмет, цели, задачи, содержание и структура дисциплины. Базовые знания, необходимые для изучения курса. Виды и формы отчетности. Рекомендуемые учебные пособия, основная и дополнительная литература по дисциплине..

1.2. Основы модулярной арифметики

Алгоритмы, их сложность и классификация. Алгоритм деления с остатком. Наибольший общий делитель. Алгоритм Евклида. Расширенный алгоритм Евклида и его обобщение. Простые и взаимно простые числа. Теорема Ферма. Теорема Эйлера. Разложение чисел на простые множители. Функция Эйлера. Сравнения и их основные свойства. Китайская теорема об остатках. Классы вычетов. Сравнения первой степени и системы сравнений первой степени. Символы Лежандра и Якоби. Криптосистемы, основанные на модулярной арифметике.

1.3. Эллиптические кривые

Основные определения. Групповая структура. Эллиптические кривые над кольцами и полями..

2. Теоретико-числовые методы

2.1. Простые числа и факторизация целых чисел

Решето Эратосфена. Критерий Вильсона. Тесты проверки простоты чисел. Алгоритмы построения простых чисел. Постановка задачи факторизации целых чисел. Детерминированные и вероятностные алгоритмы факторизации целых чисел. Метод пробного деления. Метод Ферма. Метод Лемана. Метод Полларда-Флойда. Частные случаи разложения на множители и их оптимизация. Метод Крайчика. Метод непрерывных дробей. Методы линейного и квадратичного решета.

2.2. Дискретное логарифмирование

Постановка задачи дискретного логарифмирования. Метод согласования. Алгоритм Полига-Хеллмана. Метод Полларда. Алгоритм вычисления индексов..

3. Применение теоретико-числовых методов в криптографии

3.1. Асимметричные криптосистемы

Криптографическая система RSA. Выбор ее параметров. Взаимосвязь между секретными параметрами системы. Условия на выбор простых сомножителей модуля шифрования. Выбор экспонент зашифрования и расшифрования. Атаки на систему RSA. Эллиптические кривые над конечным полем. Криптосистемы на эллиптических кривых: кодирование и дискретное логарифмирование, ключевой обмен, шифрование, электронная подпись..

3.3. Темы практических занятий

1. Криптографическая система RSA;
2. Проверка простоты чисел;
3. Сравнения;
4. Расширенный алгоритм Евклида;
5. Алгоритмы и их сложность;

6. Алгоритмы факторизации целых чисел;
7. Методы дискретного логарифмирования;
8. Криптосистемы на эллиптических кривых.

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 "Теоретико-числовые основы "
2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Теоретико-числовые методы"
3. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Применение теоретико - числовых методов в криптографии"

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:					
достижения в теоретико-числовой области математики, используемые при решении задач защиты информации	ОПК-2(Компетенция)	+			Контрольная работа/Контрольная работа №1 Основы модулярной арифметики
алгоритмы факторизации целых чисел и дискретного логарифмирования	ПК-10(Компетенция)		+		Контрольная работа/Контрольная работа №2. Простые числа и факторизация целых чисел
Уметь:					
определять требования к параметрам криптографических систем защиты информации	ОПК-2(Компетенция)	+	+		Контрольная работа/Контрольная работа №3. Дискретное логарифмирование
применять теоретико-числовые методы для оценки стойкости криптографических систем	ПК-10(Компетенция)			+	Контрольная работа/Контрольная работа №4 Группы точек эллиптических кривых.

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: Письменная работа

1. Контрольная работа №1 Основы модулярной арифметики (Контрольная работа)
2. Контрольная работа №2. Простые числа и факторизация целых чисел (Контрольная работа)
3. Контрольная работа №3. Дискретное логарифмирование (Контрольная работа)
4. Контрольная работа №4 Группы точек эллиптических кривых. (Контрольная работа)

Балльно-рейтинговая структура дисциплины является приложением А.

4.2 Промежуточная аттестация по дисциплине

Зачет с оценкой (Семестр №6)

Оценка определяется в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ» на основании семестровой и зачетной 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. Василенко, О. Н. Теоретико-числовые алгоритмы в криптографии / О. Н. Василенко, Ин-т проблем информационной безопасности МГУ . – М. : МЦНМО, 2003 . – 328 с. - ISBN 5-940571-03-4 .;
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. 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 .;
4. Лось, А. Б. Криптографические методы защиты информации : учебник для академического бакалавриата вузов по инженерно-техническим направлениям и специальностям / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков, Нац. исслед. ун-т "Высшая школа экономики" . – 2-е изд., испр . – М. : Юрайт, 2018 . – 473 с. – (Бакалавр. Академический курс) . - ISBN 978-5-534-01530-0 .;
5. Авдошин С. М., Набебин А. А.- "Дискретная математика. Модулярная алгебра, криптография, кодирование", Издательство: "ДМК Пресс", Москва, 2017 - (352 с.) https://e.lanbook.com/book/93575.

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. **Электронные ресурсы издательства Springer** - https://link.springer.com/
5. **База данных Web of Science** - http://webofscience.com/
6. **База данных Scopus** - http://www.scopus.com
7. **ЭБС "Консультант студента"** - http://www.studentlibrary.ru/
8. **Журнал Science** - https://www.sciencemag.org/
9. **Электронная библиотека МЭИ (ЭБ МЭИ)** - http://elib.mpei.ru/login.php
10. **Информационно-справочная система «Кодекс/Техэксперт»** - Http:\\proinfosoft.ru; http://docs.cntd.ru/
11. **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	М-511, Учебная аудитория	парта, стол преподавателя, стул, доска меловая
	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 промежуточной аттестации	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
	А-317, Учебная аудитория	парта со скамьей, стол преподавателя, 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
	К-307, Учебная лаборатория "Открытое программное обеспечение"	стол преподавателя, стол компьютерный, стол учебный, стул, вешалка для одежды, тумба, компьютерная сеть с выходом в Интернет, мультимедийный проектор, экран, доска маркерная, сервер, компьютер персональный, кондиционер
	К-302, Учебная лаборатория	стол преподавателя, стол компьютерный, стул, мультимедийный

	"Информационно-аналитические технологии"	проектор, экран, доска маркерная, сервер, компьютер персональный, кондиционер
Помещения для консультирования	М-511, Учебная аудитория	парта, 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

Теоретико-числовые методы криптографии

(название дисциплины)

6 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

КМ-1 Контрольная работа №1 Основы модулярной арифметики (Контрольная работа)

КМ-2 Контрольная работа №2. Простые числа и факторизация целых чисел (Контрольная работа)

КМ-3 Контрольная работа №3. Дискретное логарифмирование (Контрольная работа)

КМ-4 Контрольная работа №4 Группы точек эллиптических кривых. (Контрольная 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	Теоретико - числовые основы					
1.1	Введение		+			
1.2	Основы модулярной арифметики		+			
1.3	Эллиптические кривые				+	
2	Теоретико-числовые методы					
2.1	Простые числа и факторизация целых чисел			+	+	
2.2	Дискретное логарифмирование			+	+	
3	Применение теоретико-числовых методов в криптографии					
3.1	Асимметричные криптосистемы					+
		Вес КМ, %:	25	25	25	25