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
МАТЕМАТИЧЕСКИЕ ОСНОВЫ КРИПТОЛОГИИ

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Вариативная**
№ дисциплины по учебному плану:	**Б1.В.09.03.01**
Трудоемкость в зачетных единицах:	**6 семестр - 4;**
Часов (всего) по учебному плану:	**144 часа**
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 - 111,7 часов;**
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 2019

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, применяемых при синтезе и анализе современных криптографических систем

Задачи дисциплины

- обучение современным достижениям в области математики, и используемым для криптографической защиты информации;
- освоение терминологии и математических основ для изучения современных криптографических систем и протоколов;
- приобретение навыков применения математических 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: - теоретико-числовые основы, используемые для защиты информации; - алгебраические основы, используемые для защиты информации. уметь: - формулировать задачу и искать пути ее решения; - применять математические методы для решения задач обеспечения информационной безопасности.

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 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	Теоретико-числовые основы криптологии	48	6	6	-	8	-	-	-	-	-	34	-	***Подготовка к аудиторным занятиям:*** Проработка лекции, изучение литературы
1.1	Введение.	5		1	-	-	-	-	-	-	-	4	-	***Подготовка к текущему контролю:***
1.2	Тема 1. Основы модулярной арифметики.	21		2	-	4	-	-	-	-	-	15	-	Повторение материала по разделу "Теоретико-числовые основы криптологии" ***Подготовка к практическим занятиям:***
1.3	Тема 2. Генерация простых чисел, факторизация целых чисел и задача дискретного логарифмирования.	22		3	-	4	-	-	-	-	-	15	-	Изучение материала по разделу "Теоретико-числовые основы криптологии" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Теоретико-числовые основы криптологии" ***Изучение материалов литературных источников:*** [1], Гл.1,5,6 [3], ГЛ. 1 [4], Гл. 9, 13 [7], Гл. 1-6
2	Алгебраические основы криптологии	78		10	-	8	-	-	-	-	-	60	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Алгебраические основы криптологии" ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Подготовка домашнего задания:*** Подготовка домашнего задания направлена
2.1	Тема 3. Алгебраические системы.	19		2	-	2	-	-	-	-	-	15	-	
2.2	Тема 4. Элементы теории конечных групп.	19		2	-	2	-	-	-	-	-	15	-	

2.3	Тема 5. Элементы теории конечных полей, многочленов и эллиптических кривых над конечными полями.	19		2	-	2	-	-	-	-	-	15	-	на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Алгебраические основы криптологии" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. ***Подготовка к контрольной работе:*** Изучение материалов по разделу Алгебраические основы криптологии и подготовка к контрольной работе ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Алгебраические основы криптологии" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Алгебраические основы криптологии" ***Изучение материалов литературных источников:*** [2], Гл.2,3 [5], Гл.2 [6], Гл. 14 [7], Гл. 7-9
2.4	Тема 6. Элементы криптографических приложений теории булевых функций.	21		4	-	2	-	-	-	-	-	15	-	
	Зачет с оценкой	18.0		-	-	-	-	-	-	-	0.3	-	17.7	
	Всего за семестр	**144.0**		**16**	-	**16**	-	-	-	-	**0.3**	**94**	**17.7**	
	Итого за семестр	**144.0**		**16**	-	**16**	-		-		**0.3**	**111.7**		

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 криптологии

1.1. Введение.

Предмет, цели, задачи, содержание и структура дисциплины, математические основы криптологии (МОК). Базовые знания, необходимые для изучения курса. Виды и формы отчетности. Рекомендуемые учебные пособия основной и дополнительной литературы по дисциплине..

1.2. Тема 1. 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. Тема 2. Генерация простых чисел, факторизация целых чисел и задача дискретного логарифмирования.

Постановка задач. Тесты проверки простоты. Генерация простых чисел в ГОСТ Р 34.10-94. Методы и алгоритмы факторизации. Детерминированные и вероятностные методы дискретного логарифмирования..

2. Алгебраические основы криптологии

2.1. Тема 3. Алгебраические системы.

Алгебраические операции. Полугруппы, моноиды, группы. Подгруппы, нормальные делители, фактор – группы, гомоморфизмы и изоморфизмы групп. Теорема о гомоморфизмах. Абелевы группы. Кольца. Гомоморфизмы и идеалы колец. Типы колец. Поля. Простые поля. Поля Галуа..

2.2. Тема 4. Элементы теории конечных групп.

Теоремы Лагранжа и Кэли. Симметрическая и знакопеременная группы. Группы подстановок. Орбиты и стабилизаторы. Лемма Бернсайда. Прямое произведение (сумма) групп и подгрупп. Циклические и примарные циклические группы. Строение конечной абелевой группы..

2.3. Тема 5. Элементы теории конечных полей, многочленов и эллиптических кривых над конечными полями.

Векторные пространства над полями. Расширения полей и порядки конечных полей. Поля разложения. Строение конечных полей. Полиномы над конечными полями. Рекуррентные последовательности над конечными полями. Элементы теории эллиптических кривых над конечными полями. Группа точек эллиптической кривой. Криптосистемы на эллиптических кривых..

2.4. Тема 6. Элементы криптографических приложений теории булевых функций.

Основные понятия и определения. Числовые и метрические характеристики. Спектры Фурье и Уолша –Адамара. Классификация булевых функций. Криптографические свойства булевых функций..

3.3. Темы практических занятий

1. 3.Обоснование корректности криптосистем, основанных на модулярной арифметике;
2. 4.Методы генерации простых чисел. Факторизация целых чисел;
3. 5.Детерминированные и вероятностные методы дискретного логарифмирования;
4. 6.Алгебраические операции. Полугруппы, моноиды, группы. Подгруппы, нормальные делители, фактор – группы, гомоморфизмы и изоморфизмы групп;
5. 7.Симметрическая и знакопеременная группы и их базисы. Представление подстановок в виде произведения независимых циклов. Группы подстановок. Орбиты и стабилизаторы;
6. 8.Решение комбинаторных задач с помощью леммы Бернсайда;
7. 9.Циклические группы и их образующие. Изучение конечных абелевых групп заданного порядка;
8. 11.Неприводимые многочлены над конечными полями. Кольцо многочленов и фактор-кольцо кольца многочленов по неприводимому многочлену. Примитивные многочлены;
9. 12.Рекуррентные последовательности над конечными полями и их периодичность. Максимальные линейные рекуррентные последовательности;
10. 13.Группа точек эллиптической кривой над конечным полем и действия над ними. Примеры шифрования, кодирования и декодирования текста;
11. 14.Криптографические протоколы на эллиптических кривых. Ключевой обмен и алгоритм электронной подписи;
12. 15.Числовые и метрические характеристики булевых функций. Нахождение спектров Фурье и Уолша –Адамара. Нелинейность булевых функций;
13. 16.Классификация булевых функций. Подсчет числа классов булевых функций относительно различных групп преобразований их области определения;
14. 2.Сравнения и их основные свойства. Операции в классах вычетов. Решение системы сравнений первой степени;
15. 10.Кольца. Гомоморфизмы и идеалы колец. Типы колец. Поля. Простые поля. Поля Галуа;
16. 1.Алгоритм деления с остатком. Наибольший общий делитель. Алгоритм Евклида. Расширенный алгоритм Евклида и его обобщение.

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 криптологии"
2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Алгебраические основы криптологии"

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	
Знать:				
алгебраические основы, используемые для защиты информации	ОПК-2(Компетенция)	+		Контрольная работа/Контрольная работа №2. Факторизация и дискретное логарифмирование
теоретико-числовые основы, используемые для защиты информации	ОПК-2(Компетенция)	+		Контрольная работа/Контрольная работа №1 Основы модулярной арифметики
Уметь:				
применять математические методы для решения задач обеспечения информационной безопасности	ОПК-2(Компетенция)		+	Контрольная работа/Контрольная работа №3. Абелевы группы и вычисления в конечных полях
формулировать задачу и искать пути ее решения	ОПК-2(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. Факторизация и дискретное логарифмирование (Контрольная работа)
3. Контрольная работа №3. Абелевы группы и вычисления в конечных полях (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. 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 .;
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. Фомичев, В. М. Криптографические методы защиты информации: [в 2 ч.]. Ч. 1.: Математические аспекты : учебник для академического бакалавриата вузов по инженерно-техническим направлениям / В. М. Фомичев, Д. А. Мельников ; ред. В. М. Фомичев . – М. : Юрайт, 2018 . – 209 с. – (Бакалавр. Академический курс) . - ISBN 978-5-9916-7089-0 . - ISBN 978-5-9916-7088-3 .;

6. Гашков С. Б.- "Дискретная математика. Учебник для вузов", Издательство: "Лань", Санкт-Петербург, 2022 - (456 с.)
https://e.lanbook.com/book/193306;
7. 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.

5.3 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. **Электронная библиотека МЭИ (ЭБ МЭИ)** - http://elib.mpei.ru/login.php
5. **Информационно-справочная система «Кодекс/Техэксперт»** - Http:\\proinfosoft.ru; http://docs.cntd.ru/
6. **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 "Информационно-аналитические технологии"	стол преподавателя, стол компьютерный, стул, мультимедийный проектор, экран, доска маркерная, сервер, компьютер персональный, кондиционер
Помещения для консультирования	А-317, Учебная аудитория	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

Математические основы криптологии

(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. Факторизация и дискретное логарифмирование (Контрольная работа)

КМ-3 Контрольная работа №3. Абелевы группы и вычисления в конечных полях (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 криптологии					
1.1	Введение.		+			
1.2	Тема 1. Основы модулярной арифметики.		+			
1.3	Тема 2. Генерация простых чисел, факторизация целых чисел и задача дискретного логарифмирования.			+		
2	Алгебраические основы криптологии					
2.1	Тема 3. Алгебраические системы.				+	
2.2	Тема 4. Элементы теории конечных групп.				+	
2.3	Тема 5. Элементы теории конечных полей, многочленов и эллиптических кривых над конечными полями.					+
2.4	Тема 6. Элементы криптографических приложений теории булевых функций.					+
		Вес КМ, %:	25	25	25	25