

МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Нижегородский государственный технический университет
им. Р.Е. Алексеева» (НГТУ)

Институт радиоэлектроники и информационных технологий (ИРИТ)
(Полное и сокращенное название института, реализующего данное направление)

УТВЕРЖДАЮ:

Директор института:

_____ Мякинников А.В.

подпись

ФИО

“ 10 ” 06 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.В.ОД.8 Теоретико-числовые основы криптологии
(индекс и наименование дисциплины по учебному плану)
для подготовки бакалавров

Направление подготовки: 09.03.02 Информационные системы и технологии

Направленность: Безопасность информационных систем

Форма обучения: очная

Год начала подготовки 2021

Выпускающая кафедра ИСУ

Кафедра-разработчик ИСУ

Объем дисциплины 108/3
часов/з.е

Промежуточная аттестация зачет с оценкой

Разработчик: Тимофеева О.П., к.т.н., доцент

Нижний Новгород

2021

Рабочая программа дисциплины: разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования (ФГОС ВО 3++) по направлению подготовки 09.03.02 Информационные системы и технологии, утвержденного приказом МИНОБР-НАУКИ РОССИИ от 19 сентября 2017 года № 926 на основании учебного плана принятого УМС НГТУ

протокол от __10.06.21__ №__6__

Рабочая программа одобрена на заседании кафедры протокол от 09.06.2021 № 10
Зав. кафедрой к.т.н, доцент Тимофеева О.П. _____

(подпись)

Программа рекомендована к утверждению ученым советом института ИРИТ, Протокол от
10.06.2021 № 1

Рабочая программа зарегистрирована в УМУ, регистрационный № 09.03.02 – б-41
Начальник МО _____

Заведующая отделом комплектования НТБ

(подпись)

Н.И. Кабанова

Содержание

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ.....	4
1.1 Цель освоения дисциплины.....	4
1.2 Задачи освоения дисциплины (модуля)	4
2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ.....	4
3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	5
4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ.....	7
4.1 РАСПРЕДЕЛЕНИЕ ТРУДОЁМКОСТИ ДИСЦИПЛИНЫ ПО ВИДАМ РАБОТ ПО СЕМЕСТРАМ.....	7
4.2 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ, СТРУКТУРИРОВАННОЕ ПО ТЕМАМ.....	8
5. ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ.....	10
5.1 ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ, НЕОБХОДИМЫЕ ДЛЯ ОЦЕНКИ ЗНАНИЙ, УМЕНИЙ И НАВЫКОВ И (ИЛИ) ОПЫТА ДЕЯТЕЛЬНОСТИ.....	10
5.2 ОПИСАНИЕ ПОКАЗАТЕЛЕЙ И КРИТЕРИЕВ КОНТРОЛЯ УСПЕВАЕМОСТИ, ОПИСАНИЕ ШКАЛ ОЦЕНИВАНИЯ	11
6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ.....	13
7. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ	14
7.1 ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ	14
7.2 ПЕРЕЧЕНЬ СВОБОДНО РАСПРОСТРАНЯЕМОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ	14
7.3 ПЕРЕЧЕНЬ СОВРЕМЕННЫХ ПРОФЕССИОНАЛЬНЫХ БАЗ ДАННЫХ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ.....	14
8. ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОВЗ.....	15
9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ, НЕОБХОДИМОЕ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ.....	15
10. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ОБУЧАЮЩИМСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ	17
10.1 ОБЩИЕ МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ, ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ.....	17
10.2 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ЗАНЯТИЙ ЛЕКЦИОННОГО ТИПА.....	18
10.3 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ НА ЛАБОРАТОРНЫХ РАБОТАХ.....	18
10.4 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ НА ПРАКТИЧЕСКИХ ЗАНЯТИЯХ	18
10.5 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ КОНТРОЛЬНЫХ РАБОТ	18
10.6 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО САМОСТОЯТЕЛЬНОЙ РАБОТЕ ОБУЧАЮЩИХСЯ	18
11. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ	19
11.1 ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ, НЕОБХОДИМЫЕ ДЛЯ ОЦЕНКИ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И (ИЛИ) ОПЫТА В ХОДЕ КОНТРОЛЯ ТЕКУЩЕЙ УСПЕВАЕМОСТИ.....	19
11.2 ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ, НЕОБХОДИМЫЕ ДЛЯ ОЦЕНКИ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И (ИЛИ) ОПЫТА В ХОДЕ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ.....	19

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1 Цель освоения дисциплины

Целью освоения дисциплины является развитие компетенций в области обеспечения безопасности и целостности данных, основанное на изучении математического аппарата, лежащего в основе криптографических систем защиты информации

1.2 Задачи освоения дисциплины (модуля)

Дисциплина «Теоретико-числовые основы криптологии» способствует подготовке студентов к решению следующих профессиональных задач:

1. Исследование математических зависимостей, лежащих в основе криптографических средств защиты информации
2. Исследование принципов функционирования систем защиты информации путем исследования математических основ криптографических алгоритмов, на которых они построены.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Учебная дисциплина «Теоретико-числовые основы криптологии» Б1.В.ОД.8 включена в обязательный перечень дисциплин вариативной части (формируемой участниками образовательных отношений), определяющий направленность образовательной программы. Дисциплина реализуется в соответствии с требованиями ФГОС, ОП ВО и УП, по данному направлению подготовки.

Дисциплина базируется на дисциплинах математического блока программы бакалавриата по направлению «Информационные системы и технологии». Предшествующими курсами, на которых непосредственно базируется дисциплина «Теоретико-числовые основы криптологии», являются:

- «Алгоритмы и структуры данных»,
- «Дискретная математика».

Дисциплина «Теоретико-числовые основы криптологии» является основополагающей для изучения следующих дисциплин: «Основы криптографических методов», «Теория и методология информационной безопасности».

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина «Теоретико-числовые основы криптологии» формирует компетенцию ПКС-3 совместно с дисциплинами и практиками, указанными в таблице 3.1.

Дисциплинарная часть компетенции ПКС-3 «Способен обеспечивать безопасность и целостность данных информационных систем»: способен понимать и применять на практике математические методы теории чисел, на которых базируются алгоритмы, обеспечивающие защиту и целостность данных информационных систем.

Таблица 3.1- Формирование компетенций дисциплинам

Наименование дисциплин, формирующих компетенцию совместно	Семестры, формирования дисциплины Компетенции берутся из Учебного плана по направлению подготовки бакалавра /специалиста/магистра»							
	1	2	3	4	5	6	7	8
<i>ПКС-3: Способен обеспечивать безопасность и целостность данных информационных систем</i>								
<i>Основы криптографических методов</i>								
<i>Защита программного обеспечения</i>								
<i>Теоретико-числовые основы криптологии</i>								
<i>Безопасность сетевых протоколов</i>								
<i>Защита информационных процессов в компьютерных системах и сетях</i>								
<i>Теория и методология информационной безопасности</i>								
<i>Безопасность информационных технологий</i>								
<i>Техническая защита информации</i>								
<i>Интеллектуальные системы защиты информации</i>								
<i>Защита информации в сетях передачи данных</i>								
<i>Основы построения масштабируемых сетей передачи данных</i>								
<i>Практика по получению профессиональных умений и опыта профессиональной деятельности</i>								
<i>Преддипломная практика</i>								
<i>Выполнение и защита ВКР</i>								

Таблица 3.2- Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине			Оценочные средства	
					Текущего контроля	Промежуточной аттестации
ПКС-3 Способен обеспечивать безопасность и целостность данных информационных систем	ИПКС-3.2. Обеспечивает защиту и целостность данных в информационных системах	Знать: методы и алгоритмы теории чисел	Уметь: применять методы теории чисел для решения задач защиты информации; создавать и использовать существующие алгоритмы реализации методов теории чисел	Владеть: способностью подбирать методы и алгоритмы теории чисел для решения конкретных задач криптографической защиты информации	Контрольные работы №1, 2, 3. Задания индивидуальные для каждого студента	Вопросы для устного собеседования – 26 вопросов. Задачи для решения – 8 заданий (по вариантам)

Освоение дисциплины причастно к ТФ В/03.6 (ПС 06.032 «Специалист по безопасности компьютерных систем и сетей»), решает задачу исследования принципов функционирования программных средств криптографической защиты информации.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Распределение трудоёмкости дисциплины по видам работ по семестрам

Общая трудоёмкость дисциплины составляет Знач.ед. 108 часов, распределение часов по видам работ по семестрам представлено в таблице 4.1.

Таблица 4.1 - Распределение трудоёмкости дисциплины по видам работ по семестрам для студентов очного обучения

Вид учебной работы	Трудоёмкость в час	
	Всего час.	В т.ч. по семестрам 3 сем
Формат изучения дисциплины	с использованием элементов электронного обучения	
Общая трудоёмкость дисциплины по учебному плану	108	108
1. Контактная работа:	39	39
1.1 Аудиторная работа, в том числе:	34	34
занятия лекционного типа (Л)	17	17
занятия семинарского типа (ПЗ-семинары, практ. Занятия и др)	17	17
лабораторные работы (ЛР)		
1.2 Внеаудиторная, в том числе	5	5
курсовая работа (проект) (КР/КП) (консультация, защита)		
текущий контроль, консультации по дисциплине	4	4
контактная работа на промежуточном контроле (КРА)	1	1
2. Самостоятельная работа (СРС)	69	69
реферат/эссе (подготовка)		
расчётно-графическая работа (РГР) (подготовка)		
контрольная работа	31	31
курсовая работа/проект (КР/КП) (подготовка)		
самостоятельное изучение разделов, самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям, коллоквиум и т.д.)	20	20
Подготовка к зачёту с оценкой	18	18

4.2 Содержание дисциплины, структурированное по темам

Таблица 4.2-Содержание дисциплины, структурированное по темам для студентов очного обучения

Планируемые (контролируемые) результаты освоения:код УК; ОПК; ПК и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы (час)					Вид СРС	Наименование используемых активных и интерактивных образовательных технологий	Реализация в рамках Практической подготовки (трудоемкость в часах)	Наименование разработанного Электронного курса (трудоемкость в часах)
		Контактная работа				Самостоятельная работа студентов (час)				
		Лекции (час)	Лабораторные работы (час)	Практические занятия (час)	КСР					
3 семестр										
Раздел 1. Арифметические основы криптологии										
ПКС-3 - ИПКС-3.2	Введение История возникновения криптологии, основоположники теории чисел	1								
	Тема 1.1. НОД, НОК, простые числа. Варианты алгоритма Эвклида.	2		2		4	Подготовка к лекциям [6.1.1, 6.1.2], работа над домашним заданием	Разбор конкретных ситуаций		
	Тема 1.2. Сравнения. Классы вычетов. Первообразные корни.	2		2		4	Подготовка к лекциям [6.1.1, 6.1.2], работа над домашним заданием	Разбор конкретных ситуаций		
	Тема 1.3. Системы сравнений. Китайский алгоритм остатков.	2		3		4	Подготовка к лекциям [6.1.1, 6.1.2], работа над домашним заданием	Разбор конкретных ситуаций		
	Тема 1.4. Дискретный логарифм. Символы Лежандра и Якоби.	2		3		12	Подготовка к лекциям [6.1.1, 6.1.2], работа над домашним заданием. Подготовка к контрольной работе.	Разбор конкретных ситуаций		
	Тема 1.5. Математические принципы работы криптосистемы RSA, атаки на RSA, основанные на математическом подходе	2								

Планируемые (контролируемые) результаты освоения:код УК; ОПК; ПК и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы (час)					Вид СРС	Наименование используемых активных и интерактивных образовательных технологий	Реализация в рамках Практической подготовки (трудоемкость в часах)	Наименование разработанного Электронного курса (трудоемкость в часах)
		Контактная работа				Самостоятельная работа студентов (час)				
		Лекции (час)	Лабораторные работы (час)	Практические занятия (час)	КСР					
	Итого по 1 разделу	11		10	2	24				
Раздел 2. Алгебраические основы криптологии										
ПКС-3 - ИПКС-3.2	Тема 2.1. Группы. Порядки элементов в группе.	1		2		2	Подготовка к лекциям [6.1.1, 6.1.3], работа над домашним заданием	Разбор конкретных ситуаций		
	Тема 2.2. Кольца и поля.	1				2	Подготовка к лекциям [6.1.1, 6.1.4], работа над домашним заданием	Разбор конкретных ситуаций		
	Тема 2.3. Многочлены над полем. Неприводимые многочлены.	1		2		10	Подготовка к лекциям [6.1.1, 6.1.5], работа над домашним заданием. Подготовка к контрольной работе.	Разбор конкретных ситуаций		
	Итого по 2 разделу	3		4	1	14				
Раздел 3. Эллиптические кривые										
ПКС-3 - ИПКС-3.2	Тема 3.1. Эллиптические кривые над полем вещественных чисел.	1				2	Подготовка к лекциям [6.1.1, 6.1.2], работа над домашним заданием	Разбор конкретных ситуаций		
	Тема 3.2. Эллиптические кривые над конечными полями.	2		3		11	Подготовка к лекциям [6.1.1, 6.1.2], работа над домашним заданием. Подготовка к контрольной работе.	Разбор конкретных ситуаций		
	Итого по 3 разделу	3		3	1	13				
	Подготовка к зачёту с оценкой				1	18				
	Итого за семестр	17		17	5	69				

5. ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ.

5.1 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности

Для выполнения процедур оценивания составлен фонд оценочных средств, содержащий материалы для оценивания знаний, умений и навыков студентов для текущего контроля и промежуточной аттестации.

1. Задания контрольной работы №1:
 - Найти НОД и его линейное разложение: $au + bv = (a, b)$
 - Определить функцию Эйлера: $\varphi(b)$
 - Сформировать полную и приведенную системы вычетов: $Z_m; U(m)$
 - Найти обратный элемент: U_b в Z_p
 - Решить линейное сравнение: $ax \equiv b \pmod{p}$

Параметры заданий (a, b, m, p) выдаются каждому студенту индивидуально.

2. Задания контрольной работы №2:
 - Определить вычет: $a^{52782} \pmod{m}$
 - Решить степенное сравнение: $x^a \equiv q \pmod{p}$
 - Найти символ Лежандра: $\left(\frac{m}{q}\right)$

Параметры заданий (a, m, p, q) выдаются каждому студенту индивидуально.

3. Задания контрольной работы №3:
 - Найти НОД многочленов: $(f(X), g(X))$:
 - $f(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + a_4X^4 + a_5X^5$
 - $g(X) = b_0 + b_1X + b_2X^2 + b_3X^3 + b_4X^4$
 - $a_i, b_j \in F_2, \quad i = \overline{0,5}, \quad j = \overline{0,4}$
 - Найти все точки эллиптической кривой $E_p(a, b)$: $Y^2 = X^3 + aX + b$
 - Найти сумму двух точек эллиптической кривой $P(x_1, y_1), Q(x_2, y_2)$

Параметры заданий $(a, b, p, \text{коэффициенты многочленов})$ выдаются каждому студенту индивидуально.

4. Примерный перечень вопросов для зачета с оценкой:
 - Дать определение группы, абелевой группы, привести примеры.
 - Что такое порядок элемента в группе? (рассмотреть группы по сложению и умножению)
 - Какая группа называется циклической?
 - Как произвести разложение группы на подгруппы? (рассмотреть группы по сложению и умножению)
 - Как формируются смежные классы для подгруппы? (рассмотреть группы по сложению и умножению)
 - Дать определение кольца, привести примеры
 - Дать определение поля, поля Галуа. Привести примеры

- Что такое область целостности?
- Как задать многочлен над полем?
- Что такое неприводимый многочлен над полем?

Комплект оценочных средств является неотъемлемой частью ФОС и хранится на кафедре «Информатика и системы управления».

5.2 Описание показателей и критериев контроля успеваемости, описание шкал оценивания

Для оценки знаний, умений, навыков и формирования компетенции по дисциплине применяется **балльно-рейтинговая и традиционная** системы контроля и оценки успеваемости студентов.

В основу балльно-рейтинговой системы положены принципы, в соответствии с которыми формирование рейтинга студента осуществляется в ходе текущего, промежуточного контроля и промежуточной аттестации знаний.

Таблица 5.1 - При текущем контроле (контрольные недели) и оценке выполнения контрольных работ

Шкала оценивания	Экзамен (зачет с оценкой)
$40 < R \leq 50$	Отлично
$30 < R \leq 40$	Хорошо
$20 < R \leq 30$	Удовлетворительно
$0 < R \leq 20$	Неудовлетворительно

При промежуточном контроле успеваемость студентов оценивается по четырехбалльной системе «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Таблица 5.2–Критерии оценивания результата обучения по дисциплине и шкала оценивания

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Критерии оценивания результатов обучения			
		Оценка «неудовлетворительно» / «не зачтено» 0-59% от max рейтинговой оценки контроля	Оценка «удовлетворительно» / «зачтено» 60-74% от max рейтинговой оценки контроля	Оценка «хорошо» / «зачтено» 75-89% от max рейтинговой оценки контроля	Оценка «отлично» / «зачтено» 90-100% от max рейтинговой оценки контроля
ПКС-3. Способен проводить разработку и анализ объектов информационной безопасности	ИПКС-3.2. Разрабатывает объекты информационной безопасности	Изложение учебного материала бессистемное, неполное, не способен использовать математический аппарат при построении алгоритмов создания криптосистем для обеспечения информационной безопасности.	Фрагментарные, поверхностные знания математического аппарата; фрагментальное использование математических закономерностей для решения отдельных задач, неспособность создавать алгоритмы криптографии для обеспечения информационной безопасности.	Знает математический аппарат, лежащий в основе алгоритмов криптографии; применяет на практике математический аппарат при построении алгоритмов создания криптосистем; испытывает затруднения использовании криптографических алгоритмов для обеспечения информационной безопасности..	Имеет глубокие системные знания математического аппарата, лежащего в основе алгоритмов криптографии; применяет на практике математический аппарат при построении алгоритмов создания криптосистем для обеспечения информационной безопасности; способен делать обоснованные выводы, проводить анализ результатов работы.

Таблица 5.3 - Критерии оценивания

Оценка	Критерии оценивания
Высокий уровень «5» (отлично)	оценку « отлично » заслуживает студент, освоивший знания, умения, компетенции и теоретический материал без пробелов; выполнивший все задания, предусмотренные учебным планом на высоком качественном уровне; практические навыки профессионального применения освоенных знаний сформированы.
Средний уровень «4» (хорошо)	оценку « хорошо » заслуживает студент, практически полностью освоивший знания, умения, компетенции и теоретический материал, учебные задания не оценены максимальным числом баллов, в основном сформировал практические навыки.
Пороговый уровень «3» (удовлетворительно)	оценку « удовлетворительно » заслуживает студент, частично с пробелами освоивший знания, умения, компетенции и теоретический материал, многие учебные задания либо не выполнил, либо они оценены числом баллов близким к минимальному, некоторые практические навыки не сформированы.
Минимальный уровень «2» (неудовлетворительно)	оценку « неудовлетворительно » заслуживает студент, не освоивший знания, умения, компетенции и теоретический материал, учебные задания не выполнил, практические навыки не сформированы.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

- 6.1.1. Вычислительно сложные задачи теории чисел : Учеб.пособие / Е. А. Гречников [и др.]; МГУ им.М.В.Ломоносова. - М.: Изд-во МГУ, 2012.-310 с.
- 6.1.2. Мартынов, Л. М. Алгебра и теория чисел для криптографии : учебное пособие / Л. М. Мартынов. — Санкт-Петербург : Лань, 2020. — 456 с. — ISBN 978-5-8114-4424-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/140740>

6.2 Справочно-библиографическая литература

— учебники и учебные пособия

- 6.1.3. Мартынов, Л. М. Алгебра для криптографии : учебное пособие / Л. М. Мартынов. — Омск : ОмГУПС, [б. г.]. — Часть 1 — 2015. — 154 с. — ISBN 978-5-949-41131-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/129189>
- 6.1.4. Мартынов, Л. М. Алгебра для криптографии : учебное пособие / Л. М. Мартынов. — Омск : ОмГУПС, [б. г.]. — Часть 2 — 2015. — 150 с. — ISBN 978-5-949-41132-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/129188>
- 6.1.5. Мартынов, Л. М. Алгебра для криптографии : учебное пособие / Л. М. Мартынов. — Омск : ОмГУПС, [б. г.]. — Часть 3 — 2018. — 83 с. — ISBN 978-5-949-41189-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/129190> (дата обращения: 17.11.2021)

6.3 Перечень журналов по профилю дисциплины:

Использование журналов не предусмотрено при изучении дисциплины.

6.4 Методические указания, рекомендации и другие материалы к занятиям

Методические указания по выполнению практических работ по дисциплине «Теоретико-числовые основы криптологии» отправляются на электронные адреса групп.

- 6.1.6. Метод. указания к ауд. работе по дисциплине «Теоретико-числовые основы криптологии» для студентов направления подготовки 09.03.02 «Информационные системы и

технологии» дневной формы обучения / НГТУ; Сост.: О.П. Тимофеева, Н.Новгород, 2021, 10 с.

- 6.1.7. Метод. указания по организации самостоятельной работы по дисциплине «Теоретико-числовые основы криптологии» для студентов направления подготовки 09.03.02 «Информационные системы и технологии» дневной формы обучения / НГТУ; Сост.: О.П. Тимофеева, Н.Новгород, 2020, 15 с.

7. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Учебный процесс по дисциплине обеспечен необходимым комплектом свободно распространяемого программного обеспечения (состав по дисциплине определен в настоящей РПД и подлежит обновлению при необходимости).

7.1 Перечень информационных справочных систем

Таблица 7.1 -Перечень электронных библиотечных систем

№	Наименование ЭБС	Ссылка к ЭБС
1	Лань	https://e.lanbook.com/
2	Юрайт	https://biblio-online.ru/

7.2 Перечень свободно распространяемого программного обеспечения

Таблица 7.2 – Программное обеспечение, используемое студентами очного обучения

Программное обеспечение, используемое в университете на договорной основе	Программное обеспечение свободного распространения
-	Adobe Acrobat Reader (https://acrobat.adobe.com/ru/ru/acrobat/pdf-reader.html)
	Linux (https://www.linux.com/)
	OpenOffice (FreeWare) https://www.openoffice.org/ru/
	JDK 8 и выше (https://adoptopenjdk.net/)
	Фреймворк Java Spring 5 (https://spring.io/projects/spring-framework)
	Eclipse (https://www.eclipse.org/)
	IntelliJ Idea (https://www.jetbrains.com/ru-ru/idea/)
	git (https://git-scm.com/), github (https://github.com/)
	Maven (https://maven.apache.org/), Gradle (https://gradle.org/)
	Редактор блок-схем (https://app.diagrams.net/)

7.3 Перечень современных профессиональных баз данных и информационных справочных систем

В таблице 7.4 указан перечень профессиональных баз данных и информационных справочных систем, к которым обеспечен доступ (удаленный доступ). Данный перечень подлежит обновлению в соответствии с требованиями ФГОС ВО.

В данном разделе могут быть приведены ресурсы (ссылки на сайты), на которых можно найти полезную для курса информацию, в т.ч. статистические или справочные данные, учебные материалы, онлайн курсы и т.д.

Таблица 7.4– Перечень современных профессиональных баз данных и информационных справочных систем

№	Наименование профессиональной базы данных, информационно-справочной системы	Доступ к ресурсу (удаленный доступ с указанием ссылки/доступ из локальной сети университета)
1	2	3
1	База данных стандартов и регламентов РОССТАНДАРТ	https://www.rst.gov.ru/portal/gost/home/standarts
2	Перечень профессиональных баз данных и информационных справочных систем	https://cyberpedia.su/21x47c0.html
3	Каталог паттернов проектирования	https://refactoring.guru/ru/design-patterns/catalog

8. ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОВЗ

В таблице 8.1 указан перечень образовательных ресурсов, имеющих формы, адаптированные к ограничениям их здоровья, а также сведения о наличии специальных технических средств обучения коллективного и индивидуального пользования. При заполнении таблицы может быть использована информация, размещенная в подразделе «Доступная среда» специализированного раздела сайта НГТУ «Сведения об образовательной организации» <https://www.nntu.ru/sveden/accenv/>

Таблица 8.1 - Образовательные ресурсы для инвалидов и лиц с ОВЗ

№	Перечень образовательных ресурсов, приспособленных для использования инвалидами и лицами с ОВЗ	Сведения о наличии специальных технических средств обучения коллективного и индивидуального пользования
1	ЭБС «Консультант студента»	озвучка книг и увеличение шрифта
2	ЭБС «Лань»	специальное мобильное приложение - синтезатор речи, который воспроизводит тексты книг и меню навигации
3	ЭБС «Юрайт»	версия для слабовидящих

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ, НЕОБХОДИМОЕ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Для контактной и самостоятельной работы обучающихся выделены помещения, оснащённые компьютерной техникой с подключением к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации:

- зал электронно-информационных ресурсов (ауд. 2210 – 11 компьютеров, ауд. 6119 – 9 компьютеров);
- читальный зал открытого доступа (ауд. 6162 – 2 компьютера);
- ауд. 2303, 2202, оборудованные Wi-Fi.

Перечень материально-технического обеспечения, необходимого для реализации программы бакалавриата для студентов очного обучения, включает в себя компьютерные классы

1. Ауд. 4408 кафедры «Информатика и системы управления» - лаборатория Информационных технологий.

Компьютеры, оснащенные необходимым оборудованием, техническими и электронными средствами обучения и контроля знаний студентов.

- 8 рабочих мест на базе тонких клиентов DellWise,
- мультимедийный проектор BenQ PB6240,
- ноутбук Lenovo V130-151KB,
- стенд для изучения автоматических систем управления на базе блока MyRio с FPGA под управлением LabView.

Пакеты ПО (лицензионное):

- Dr.Web (с/н H365-W77K-B5HP-N346 от 31.05.2021).

Пакеты ПО (распространяемое по свободной лицензии):

- Apache OpenOffice;
- Linux Ubuntu 20.04 (<https://releases.ubuntu.com/20.04/>)
- git (<https://git-scm.com/>)
- Microsoft Visual Studio 2017 Community Edition (<https://visualstudio.microsoft.com/ru/vs/community/>)

Также, для самостоятельной работы обучающихся выделены помещения, оснащённые компьютерной техникой с подключением к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации:

Таблица 9.1 - Оснащенность аудиторий и помещений для самостоятельной работы студентов по дисциплине

№	Наименование аудиторий и помещений для самостоятельной работы	Оснащенность аудиторий помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
1	1	2	3
1	6421 учебная аудитория для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации; г. Нижний Новгород, Казанское ш., 12	Комплект демонстрационного оборудования: • ПК, с выходом на мультимедийный проектор, на базе AMD Athlon 2.8 ГГц, 4 Гб ОЗУ, 250 Гб HDD, монитор 19" – 1 шт. • Мультимедийный проектор Epson- 1 шт; • Экран – 1 шт.; Набор учебно-наглядных пособий	• Microsoft Windows7 (подписка DreamSpark Premium, договор №Tr113003 от 25.09.14) • Gimp 2.8 (свободное ПО, лицензия GNU GPLv3); • Microsoft Office Professional Plus 2007 (лицензия № 42470655); • Open Office 4.1.1 (свободное ПО, лицензия Apache License 2.0) • Adobe Acrobat Reader (FreeWare); • 7-zip для Windows (свободно распространяемое ПО, лицензия GNU LGPL); - Dr.Web (Сертификат №EL69-RV63-YMBJ-N2G7 от 14.05.19).
	6543 компьютерный класс - помещение для СРС, курсового проектирования (выполнения курсовых работ), г. Нижний Новгород, Казанское ш., 12)	• Проектор Accer – 1 шт; • ПК на базе IntelCoreDuo 2.93 ГГц, 2 Гб ОЗУ, 320 Гб HDD, монитор Samsung 19" – 11 шт.. ПК подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду университета	• Microsoft Windows 7 (подписка DreamSpark Premium, договор № Tr113003 от 25.09.14); • Microsoft Office (лицензия № 43178972); • Adobe Design Premium CS 5.5.5 (лицензия № 65112135); • Adobe Acrobat Reader (FreeWare); • 7-zip для Windows (свободно распространяемое ПО, лицензия GNU LGPL); • Dr.Web (Сертификат №EL69-RV63-YMBJ-N2G7 от 14.05.19) • КонсультантПлюс(ГПД № 0332100025418000079 от 21.12.2018); - Gimp 2.8 (свободное ПО, лицензия GNU GPLv3)

10. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ОБУЧАЮЩИМСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

10.1 Общие методические рекомендации для обучающихся по освоению дисциплины, образовательные технологии

Дисциплина реализуется посредством проведения контактной работы с обучающимися (включая проведение текущего контроля успеваемости), самостоятельной работы обучающихся и промежуточной аттестации.

При преподавании дисциплины «Теоретико-числовые основы криптологии», используются современные образовательные технологии, позволяющие повысить активность студентов при освоении материала курса и предоставить им возможность эффективно реализовать часы самостоятельной работы.

Весь лекционный материал курса сопровождается компьютерными презентациями, в которых наглядно преподносятся материал различных разделов курса и что дает возможность обсудить материал со студентами во время чтения лекций, активировать их деятельность при освоении материала. Электронные материалы лекций в период дистанционного обучения отправляются по электронной почте на адреса групп и могут быть получены до чтения лекций и проработаны студентами в ходе самостоятельной работы.

На лекциях, практических занятиях реализуются интерактивные технологии, приветствуются вопросы и обсуждения, используется личностно-ориентированный подход, технология работы в малых группах, что позволяет студентам проявить себя, получить навыки самостоятельного изучения материала, выравнивать уровень знаний в группе.

Все вопросы, возникшие при самостоятельной работе над домашним заданием подробно разбираются на практических занятиях и лекциях. Проводятся индивидуальные и групповые консультации с использованием современных информационных технологий: электронная почта, мессенджеры, Zoom, Discord.

Иницируется активность студентов, поощряется задание любых вопросов по материалу, практикуется индивидуальный ответ на вопросы студента, рекомендуются методы успешного самостоятельного усвоения материала в зависимости от уровня его базовой подготовки.

Для оценки знаний, умений, навыков и уровня сформированности компетенции применяется балльно-рейтинговая система контроля и оценки успеваемости студентов в процессе текущего контроля.

Промежуточная аттестация проводится в форме зачета с оценкой с учетом текущей успеваемости.

Результат обучения считается сформированным на повышенном уровне, если теоретическое содержание курса освоено полностью. При устных собеседованиях студент исчерпывающе, последовательно, четко и логически излагает учебный материал; свободно справляется с заданиями, вопросами, использует в ответе дополнительный материал. Все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты, проявляет самостоятельность при выполнении заданий.

Результат обучения считается сформированным на пороговом уровне, если теоретическое содержание курса освоено полностью. При устных собеседованиях студент последовательно, четко и логически излагает учебный материал; справляется с заданиями, вопросами, требующих применения знаний; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий.

Результат обучения считается несформированным, если студент при выполнении заданий не демонстрирует знаний учебного материала, допускает ошибки, неуверенно, с большими затруднениями выполняет задания, не демонстрирует необходимых умений, качество выполненных заданий не соответствует установленным требованиям, качество их выполнения оценено числом баллов ниже трех по оценочной системе, что соответствует допороговому уровню.

10.2 Методические указания для занятий лекционного типа

Лекционный курс предполагает систематизированное изложение основных вопросов тематического плана. В ходе лекционных занятий раскрываются базовые вопросы в рамках каждой темы дисциплины (Таблицы 4.4, 4.5, 4.6). Обозначаются ключевые аспекты тем, а также делаются акценты на наиболее сложные и важные положения изучаемого материала. Материалы лекций являются опорной основой для подготовки обучающихся к практическим занятиям и выполнения заданий самостоятельной работы, а также к мероприятиям текущего контроля успеваемости и промежуточной аттестации по дисциплине.

10.3 Методические указания по освоению дисциплины на лабораторных работах

Лабораторные работы по дисциплине не предусмотрены

10.4 Методические указания по освоению дисциплины на практических занятиях

Практические занятия представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы. Основной формой проведения практических занятий является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также решение задач и разбор примеров и ситуаций в аудиторных условиях.

Практические занятия обучающихся обеспечивают:

- проверку и уточнение знаний, полученных на лекциях;
- навыков обсуждения вопросов по учебному материалу дисциплины;
- подведение итогов занятий по рейтинговой системе, согласно технологической карте дисциплины.

10.5 Методические указания по выполнению контрольных работ

Контрольная работа по дисциплине предусмотрена учебным планом и состоит из трех частей. Решение контрольной работы способствует лучшему освоению обучающимися учебного материала, формирует практический опыт и умения по изучаемой дисциплине, способствует формированию у обучающихся готовности к самостоятельной профессиональной деятельности.

При подготовке к выполнению заданий контрольной работы рекомендуется проработка материалов лекций по каждой пройденной теме, анализ примеров решения задач, выполненных на практических занятиях и проработанных в ходе решения домашних заданий.

Типовые задания контрольной работы приведены в п.5.1.

10.6 Методические указания по самостоятельной работе обучающихся

Самостоятельная работа обеспечивает подготовку обучающегося к аудиторным занятиям и мероприятиям текущего контроля и промежуточной аттестации по изучаемой дисциплине. Результаты этой подготовки проявляются в активности обучающегося на занятиях и в качестве выполненных практических заданий и других форм текущего контроля.

При выполнении заданий для самостоятельной работы рекомендуется проработка материалов лекций по каждой пройденной теме, а также изучение рекомендуемой литературы, представленной в Разделе 6.

В процессе самостоятельной работы при изучении дисциплины студенты могут работать на компьютере в специализированных аудиториях для самостоятельной работы, указанных в Разделе 9. В аудиториях имеется доступ через информационно-телекоммуникационную сеть «Интернет» к электронной информационно-образовательной среде университета (ЭИОС) и электронной библиотечной системе (ЭБС), где в электронном виде располагаются учебные и учебно-методические материалы, которые могут быть использованы для самостоятельной работы при изучении дисциплины.

11. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

11.1 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта в ходе контроля текущей успеваемости

Для текущего контроля знаний студентов по дисциплине проводится **комплексная оценка знаний**, включающая

- решение контрольных работ (типовые задания приведены в п.5.1).

11.1.1. Типовые задания для практических занятий.

Типовые задания для практических занятий приведены в учебно-методических указаниях по проведению самостоятельной работы по дисциплине.

11.2 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта в ходе промежуточной аттестации по дисциплине

11.2.1. Защита курсового проекта/ работы

Курсовая работа не предусмотрена учебным планом

11.2.2. Зачет с оценкой для студентов очной формы обучения в 3 семестре.

Проводится в виде устного собеседования по типовым вопросам или выставляется по накопительной системе, как среднее арифметическое результатов проведенных в течение семестра контрольных работ.

Типовые вопросы для промежуточной аттестации в форме зачета с оценкой для студентов очной формы обучения:

1. Определение НОД, нахождение НОД по алгоритму Эвклида
2. Что такое каноническое разложение числа на простые множители? Какие алгоритмы вам известны?
3. Понятие вычета по модулю m . Что такое полная система вычетов, приведенная система вычетов?
4. Понятие функции Эйлера для m , алгоритм нахождения
5. Понятие обратного элемента в Zm , алгоритмы нахождения
6. Что является решением сравнения? В чем разница в решении для простого и составного m .
7. Теорема о решении системы сравнений китайским алгоритмом. Методы решения систем.
8. Что такое первообразный корень? Нахождение первообразного корня и формирование с его помощью приведенной системы вычетов
9. Что такое индекс числа? Понятие дискретного логарифма в Zm .
10. Понятие символа Лежандра и символа Якоби.
11. Дать определение группы, абелевой группы.
12. Что такое порядок элемента в группе?
13. Дать определение кольца.
14. Дать определение поля, поля Галуа. Что такое характеристика поля?
15. Как задать многочлен над полем? Степень многочлена.
16. Что такое НОД многочленов?
17. Что такое неприводимый многочлен над полем?
18. Что такое поле многочленов?
19. Дать определение эллиптической кривой над полем.
20. Пояснить смысл бесконечно удаленной точки.
21. Пояснить смысл дискриминанта эллиптической кривой.

22. Пояснить арифметические действия над точками эллиптической кривой, определенной над полем вещественных чисел.
23. Пояснить алгоритм получения точек эллиптической кривой над конечным полем.
24. Что такое порядок эллиптической кривой?
25. Что такое порядок точки на эллиптической кривой?
26. В чем состоит задача дискретного логарифмирования на эллиптических кривых?

В полном объеме оценочные средства имеются на кафедре «Информатика и системы управления». Оценочные средства могут быть получены по требованию.

УТВЕРЖДАЮ:
Директор института ИРИТ

_____ Мякинников А.В.
«__» _____ 2021 г.

Лист актуализации рабочей программы дисциплины
«Б1.В.ОД.8 Теоретико-числовые основы криптологии»
индекс по учебному плану, наименование

для подготовки бакалавров/ специалистов/ магистров

Направление: 09.03.02 Информационные системы и технологии

Направленность: Безопасность информационных систем

Форма обучения очная

Год начала подготовки: 2021

Курс 2

Семестр 3

В рабочую программу не вносятся изменения. Программа актуализирована для 2021 г. начала подготовки.

Разработчик (и): Тимофеева О.П., к.т.н., доцент
(ФИО, ученая степень, ученое звание) «__» _____ 20__ г.

Рабочая программа пересмотрена и одобрена на заседании кафедры ИСУ
_____ протокол № _____ от «__» _____ 20__ г.

Заведующий кафедрой ИСУ _____ Тимофеева О.П.

Лист актуализации принят на хранение:

Заведующий выпускающей кафедрой ИСУ _____ «__» _____ 20__ г.

Методический отдел УМУ: _____ «__» _____ 20__ г.