УТВЕРЖДАЮ:
Директор института ИРИТ

_____Мякиньков А.В.
3 июня 2024 г.

Лист актуализации рабочей программы дисциплины
«Б1.Б.16 Теоретико-числовые методы в криптографии»
индекс по учебному плану, наименование

для подготовки бакалавров/ **специалистов**/ магистров
Направление: 10.05.03 «Информационная безопасность автоматизированных систем»
Направленность: Безопасность открытых информационных систем
Форма обучения: очная
Год начала подготовки: 2024

Курс 2
Семестр 4

В рабочую программу 2023г вносятся изменения:
1) Табл.8.1 читать в следующей редакции:

№	Наименование ЭБС	Ссылка к ЭБС
1	Консультант студента	http://www.studentlibrary.ru/
2	Лань	https://e.lanbook.com/
3	Юрайт	https://biblio-online.ru/
4	TNT-ebook	https://www.tnt-ebook.ru/

2) П.9 читать в следующей редакции:
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.

Лаборатория "Информационные технологии" №4408 учебного корпуса №4 для проведения учебных занятий
Оснащенность оборудованием и техническими средствами обучения:
1. Мультимедийный проектор BenQ PB6240 - 1 шт.
2. Ноутбук Lenovo V130-151KB - 1 шт.
3. Стенд для изучения автоматических систем управления на базе блока MyRio с FPGA под управлением LabView.
4. Рабочие места на базе тонких клиентов Dell Wise - 8 шт.
5. Рабочее место студента - 40.
Программное обеспечение:
1. Dr.Web (С/н ZNFC-CR5D-5U3U-JKGP от 20.05.2024, до 30.05.25)
2. Распространяемое по свободной лицензии: Apache OpenOffice
Передаваемое ОУ на бесплатной основе в учебных целях: Microsoft Windows 10 (подписка DreamSpark Premium, договор № 0509/КМР от 15.10.18)

Мультимедийная аудитория №6421 учебно-лабораторного корпуса №6 для проведения учебных занятий

Оснащенность оборудованием и техническими средствами обучения:

1. Доска меловая – 1 шт.
3. Экран – 1 шт.
4. Мультимедийный проектор Epson X12 – 1 шт.
5. Компьютер PC MB Asus на чипсете Nvidia/AMDAthlonXII CPU 2.8Ggz/ RAM 4 Ggb/SVGAStandartGraphics +Ge-FORCE Nvidia GT210/HDD 250Ggb,SATAinterface, монитор 19", с выходом на проектор.
6. Рабочее место студента - 30
7. Рабочее место для преподавателя – 1 шт.

Программное обеспечение:

1. Windows 7 32 bit корпоративная; VL 49477S2
2. Adobe Acrobat Reader DC-Russian (беспл.)
3. Microsoft Office Professional Plus 2007 (лицензия № 42470655);
4. Dr.Web (С/н ZNFC-CR5D-5U3U-JKGP от 20.05.2024, до 30.05.25)

Программа актуализирована для 2024 г. начала подготовки.

Разработчик (и): __Капранов С.Н., к.т.н., доцент_____
(ФИО, ученая степень, ученое звание)

«_15_»_05___2024г.

Рабочая программа пересмотрена и одобрена на заседании кафедры ИБВСС протокол № _9___ от «_15_» ___05___2024_г.

И.о. заведующий кафедрой _____Ляхманов Д.А.

Лист актуализации принят на хранение:

Заведующий выпускающей кафедрой ИБВСС _____03.06. 2024г.

Методический отдел УМУ:_____03.06.2024 г.

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

Учебно-научный институт радиоэлектроники и информационных технологий (ИРИТ)
(Полное и сокращенное название института, реализующего данное направление)

УТВЕРЖДАЮ:
Директор института:
_____ Мякиньков А.В.
подпись ФИО
22 апреля 2023г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.Б.16 Теоретико-числовые методы в криптографии
(индекс и наименование дисциплины по учебному плану)
для подготовки специалистов

Направление подготовки: 10.05.03 «Информационная безопасность автоматизированных систем»

Направленность: Безопасность открытых информационных систем

Форма обучения: очная
Год начала подготовки 2022

Выпускающая кафедра ИБВСС

Кафедра-разработчик ИБВСС

Объем дисциплины 144/4
часов/з.е
Промежуточная аттестация Зачет с оценкой

Разработчик: Капранов С.Н., к.т.н., доцент

Нижний Новгород

2023

Рабочая программа дисциплины: разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования (ФГОС ВО 3++) по направлению подготовки «Информационная безопасность автоматизированных систем», утвержденного приказом МИНОБРНАУКИ РОССИИ от 26 ноября 2020 г. № 1457 на основании учебного плана, принятого УМС НГТУ

протокол от 20.04.2023 № 18.

Рабочая программа одобрена на заседании кафедры протокол от _01.04.2023_ № 4
Зав. кафедрой к.т.н, доцент Ляхманов Д.А. _____
(подпись)

Программа рекомендована к утверждению ученым советом института ИРИТ, Протокол от 21.04.2023_____ № 4

Рабочая программа зарегистрирована в УМУ, регистрационный № 10.05.03-Б-15
Начальник МО _____ Н.Р. Булгакова

Заведующая отделом комплектования НТБ _____ Н.И. Кабанина
(подпись)

Содержание

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 методы в криптографии» 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 методы в криптографии» Б1.Б.16 включена в обязательный перечень дисциплин обязательной части образовательной программы вне зависимости от ее направленности (профиля). Дисциплина реализуется в соответствии с требованиями ФГОС 3++, ОП ВО и УП, по направлению подготовки 10.05.03.

Дисциплина базируется на дисциплинах математического блока программы специалитета по направлению «Информационные системы и технологии». Предшествующими курсами, на которых непосредственно базируется дисциплина «Теоретико-числовые методы в криптографии», являются:

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

Дисциплина «Теоретико-числовые методы в криптографии» является основополагающей для изучения следующих дисциплин: «Методы и средства криптографической защиты информации».

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

Дисциплина «Теоретико-числовые методы в криптографии» формирует компетенцию ОПК-3 совместно с дисциплинами и практиками, указанными в таблице 3.1.

Таблица 3.1- Формирование компетенций дисциплинам

Наименование дисциплин, формирующих компетенцию совместно	Семестры, формирования дисциплины Компетенции берутся из Учебного плана по направлению подготовки специалиста»										
	1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*
ОПК-3 *(Способен использовать математические методы, необходимые для решения задач профессиональной деятельности)*											
Математика											
Дискретная математика											
Теоретико-числовые методы в криптографии											
Теория вероятностей и математическая статистика											
Теория информации											
Методы оптимизации											
Теория принятия решений											
Принятие решений при нечетких исходных данных											
Методы моделирования открытых информационных систем											
Государственный экзамен											

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**
ОПК-3. Способен использовать математические методы, необходимые для решения задач профессиональной деятельности	ИОПК-3.3. Применяет математические методы для решения задач защиты информации	***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)

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Распределение трудоёмкости дисциплины по видам работ по семестрам

Общая трудоёмкость дисциплины составляет 4зач.ед. 144 часа, распределение часов по видам работ 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	**144**	**144**
1. Контактная работа:	**72**	**72**
1.1 Аудиторная работа, в том числе:	**68**	**68**
занятия лекционного типа (Л)	34	34
занятия семинарского типа (ПЗ-семинары, практ. Занятия и др)	34	34
лабораторные работы (ЛР)		
1.2 Внеаудиторная, в том числе	**4**	**4**
курсовая работа (проект) (КР/КП) (консультация, защита)		
текущий контроль, консультации по дисциплине	3	3
контактная работа на промежуточном контроле (КРА)	1	1
2. Самостоятельная работа (СРС)	**72**	**72**
реферат/эссе (подготовка)		
расчётно-графическая работа (РГР) (подготовка)		
контрольная работа	33	33
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.)	39	39
Подготовка к зачёту с оценкой	-	-

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										
ОПК-3 - ИОПК-3.3	**Введение** История возникновения криптологии, основоположники теории чисел	2								
	Тема 1.1. НОД, НОК, простые числа. Варианты алгоритма Эвклида.	4		4		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.	4		4		4	Подготовка к лекциям [6.1.1, 6.1.2], работа над домашним заданием	Разбор конкретных ситуаций		

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					
	Тема 1.3. Системы сравнений. Китайский алгоритм остатков.	4		6		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.	4		6		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	4								
	Итого по 1 разделу	**22**		**20**	**1**	**24**				
Раздел 2. Алгебраические основы криптологии										

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					
ОПК-3 - ИОПК-3.3	**Тема 2.1.** Группы. Порядки элементов в группе.	2		4		2	Подготовка к лекциям [6.1.1, 6.1.3], работа над домашним заданием	Разбор конкретных ситуаций		
	Тема 2.2. Кольца и поля.	2				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.	2		4		10	Подготовка к лекциям [6.1.1, 6.1.5], работа над домашним заданием. Подготовка к кон-трольной работе.	Разбор конкретных ситуаций		
	Итого по 2 разделу	**6**		**8**	**1**	**14**				
Раздел 3. Эллиптические кривые										
ОПК-3 - ИОПК-3.3	**Тема 3.1.** Эллиптические кривые над полем вещественных чисел.	2				2	Подготовка к лекциям [6.1.1, 6.1.2], работа над домашним заданием	Разбор конкретных ситуаций		

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					
	Тема 3.2. Эллиптические кривые над конечными полями.	4		6		14	Подготовка к лекциям [6.1.1, 6.1.2], работа над домашним заданием. Подготовка к контрольной работе.	Разбор конкретных ситуаций		
	Итого по 3 разделу	**6**		**6**	**1**	**16**				
	Подготовка к зачёту с оценкой				**1**	**18**				
	Итого за семестр	**34**		**34**	**4**	**72**				

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: $ax \equiv b (\mathrm{mod} p)$

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

2. Задания контрольной работы №2:
   - Определить вычет: $a^{52782} (\mathrm{mod}\ m)$
   - Решить степенное сравнение: $x^a \equiv q (\mathrm{mod}\ p)$
   - 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)):
  - $f(X) = a_0 + a_1 X + a_2 X^2 + a_3 X^3 + a_4 X^4 + a_5 X^5$
  - $g(X) = b_0 + b_1 X + b_2 X^2 + b_3 X^3 + b_4 X^4$
  - $a_i, b_j \in F_2, \quad i = \overline{0,5}, \quad j = \overline{0,4}$
- 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*, 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 «Информационная безопасность вычислительных систем и сетей».

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<=50	Отлично
30<R<=40	Хорошо
20<R<=30	Удовлетворительно
O<R<=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 наименовани 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
ОПК-3. Способен использовать математические методы, необходимые для решения задач профессиональной деятельности	ИОПК-3.3. Применяет математические методы для решения задач защиты информации	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 : Ом ГУПС, [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 : Ом ГУПС, [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 : Ом ГУПС, [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

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 методы в криптографии» отправляются на электронные адреса групп.

6.1.6. Метод. указания к ауд. работе по дисциплине «Теоретико-числовые методы в криптографии» для студентов направления подготовки 09.03.02 «Информационные системы и технологии», 10.05.03 «Информационная безопасность автоматизированных систем» 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 методы в криптографии» для студентов направления подготовки 09.03.02 «Информационные системы и технологии», 10.05.03 «Информационная безопасность автоматизированных систем» 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	«Консультант студента - Электронная библиотека технического вуза»	http://www.studentlibrary.ru/
2	Лань	https://e.lanbook.com/
3	«Юрайт» (коллекция «Легендарные книги»)	https://urait.ru/
4	«Техэксперт» - «Нормы, правила, стандарты и законодательство России»	https://www.nntu.ru/frontend/web/ngtu/files/org_structura/library/resurvsy/tehekspert.pdf

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 и предоставляемые вузам на бесплатной основе
1. Windows 7 32 bit корпоративная VL 49477S2 2. Adobe Acrobat Reader DC-Russian (беспл.) 3. Microsoft Office Professional Plus 2007 (лицензия № 42470655); 4 Dr.Web (с/н GMN9-DSLH-G4U1-LW6H от 11.05.23 5. Распространяемое по свободной лицензии: Apache OpenOffice 6. Microsoft Windows 7 MSDN реквизиты договора - подписка DreamSpark Premium, договор № Tr113003 от 25.09.14	Пакет программ Open Office, True Conf, Браузер Google Chrome, Браузер Mozilla Firefox, Браузер Opera, McAfee Security Scan, Adobe Acrobat Reader DC, AutoCAD2013 Обеспечено подключение ПК к сети «Интернет» и доступ в электронную информационно-образовательную среду университета Передаваемое ОУ на бесплатной основе в учебных целях: ОС Windows 10 (лицензия Spark для ВУЗов)

7.3 Перечень современных профессиональных баз данных и информационных справочных систем

В таблице7.4указан 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 издательства Wiley	https://onlinelibrary.wiley.com/
2	База данных Polpred	http://www.polpred.com
3	Научная электронная библиотека ELIBRARY.RU	http://elibrary.ru
4	База данных стандартов и регламентов РОССТАНДАРТ	https://www.rst.gov.ru/portal/gost/home/standarts
5	Перечень профессиональных баз данных и информационных справочных систем	https://cyberpedia.su/21x47c0.html
6	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/ovz/.

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»	Версия для слабовидящих, прослушивание с помощью синтезатора речи
2	ЭБС «Лань»	Версия для слабовидящих, прослушивание с помощью синтезатора речи
3	«Юрайт» (коллекция «Легендарные книги»)	Версия для слабовидящих

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

Учебные аудитории для проведения занятий по дисциплине, оснащены оборудованием и техническими средствами обучения

В таблице 9 перечислены:

- учебные аудитории для проведения учебных занятий, оснащенные оборудованием и техническими средствами обучения;

- помещения для самостоятельной работы обучающихся, которые должны оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду НГТУ.

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	Учебная аудитория № 6421 учебно-лабораторного корпуса № 6 для проведения учебных занятий. 603163, Нижегородская область, г. Нижний Новгород, Казанское шоссе, д.12	1. Доска меловая – 1 шт. 3. Экран – 1 шт. 4. Мультимедийный проектор Epson X12 – 1 шт. 5. Компьютер PC MB Asus на чипсете Nvidia/AMDAthlonXII CPU 2.8Ggz/ RAM 4 Ggb/SVGAStandartGraphics +Ge-FORCE Nvidia GT210/HDD 250Ggb,SATAinterface, монитор 19”, с выходом на проектор. 6. Рабочее место студента - 74 7. Рабочее место для преподавателя – 1 шт.	1. Windows 7 32 bit корпоративная; VL 49477S2 2. Adobe Acrobat Reader DC-Russian (беспл.) 3. Microsoft Office Professional Plus 2007 (лицензия № 42470655); 4. Dr.Web (с/н GMN9-DSLH-G4U1-LW6H от 11.05.23 до 28.05.24)
2	Лаборатория «Информационные технологии» № 4408 учебного корпуса № 4 для проведения для проведения учебных занятий и обеспечения практической подготовки обучающихся. 603155, Нижегородская область, г. Нижний Новгород, ул. Минина д.28В	1. Мультимедийный проектор BenQ PB6240 - 1 шт. 2. Ноутбук Lenovo V130-151KB - 1 шт. 3. Стенд для изучения автоматических систем управления на базе блока MyRio с FPGA под управлением LabView. 4. Рабочие места на базе тонких клиентов Dell Wise - 8 шт. 5. Рабочее место студента - 40.	1. Dr.Web (с/н GMN9-DSLH-G4U1-LW6H от 11.05.23 до 28.05.24) 2. Распространяемое по свободной лицензии: Apache OpenOffice Передаваемое ОУ на бесплатной основе в учебных целях: **ОС Windows 10 (лицензия Spark для ВУЗов)**
3	Компьютерный класс № 1 - Помещение для самостоятельной работы обучающихся № 6543 учебно-лабораторного корпуса № 6 для проведения научно-исследовательской работы обучающихся, курсового и дипломного проектирования. 603163, Нижегородская область, г. Нижний Новгород, Казанское шоссе, д.12	1. Рабочие места студента, оснащенные ПК на базе Intel Core i5 с мониторами – 8 шт. 2. Рабочие места студента, оснащенные ПК на базеCore 2 Duo с мониторами –2 шт. 3. Рабочее место преподавателя, оснащенное ПК на базе Intel Core i5 с монитором – 1 шт. 4. Проектор Accer, проекционный экран – 1 шт. ПК подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду университета 5. Принтер HP LaserJet 1200 – 1 шт.	1. Microsoft Windows 7 MSDN реквизиты договора - подписка DreamSpark Premium, договор № 0509/КМР от 15.10.18 2. Бесплатное ПО: Пакет программ Open Office, True Conf, Браузер Google Chrome, Браузер Mozilla Firefox, Браузер Opera, McAfee Security Scan, Adobe Acrobat Reader DC, AutoCAD2013

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 методы в криптографии», 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, выровнять 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.

Инициируется 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.

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.

10.3Методические 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.

10.6Методические 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 4 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:

Вопросы, направленные на проверку компетенции ОПК-3:

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 «Информационная безопасность вычислительных систем и сетей». Оценочные средства могут быть получены по требованию.