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

Дзержинский политехнический институт (филиал)

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 50680B7E282BE1190F7ADAFAB67930C8
Владелец: Петровский Александр Михайлович
Действителен: с 23.12.2024 до 18.03.2026

УТВЕРЖДАЮ:
Директор института:
_____А.М. Петровский
“ 10 ”___июня_____2024г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ОД.1Математические основы криптологии
(индекс и наименование дисциплины по учебному плану)
для подготовки магистров

Направление подготовки: 09.04.02 Информационные системы и технологии

Направленность: Безопасность информационных систем

Форма обучения: очная
Год начала подготовки 2024

Выпускающая кафедра АЭМИС

Кафедра-разработчик АЭМИС

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

Разработчик: Осипов В.Н., к.т.н., доцент

Нижний Новгород

2024

Рабочая программа дисциплины: разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования (ФГОС ВО 3++) по программе магистров 09.04.02. «Информационные системы и технологии», утвержденного приказом МИНОБРНАУКИ РОССИИ от 19.09.2017 №917 на основании учебного плана принятого УС ДПИ НГТУ

протокол от 05.06.2024 № 10

Рабочая программа одобрена на заседании кафедры-разработчика РПД Автоматизация, энергетика, математика и информационные системы

протокол от 10.06.2024 № 7

Заведующий кафедрой разработчика РПД к.т.н, доцент Вадова Л.Ю.

СОГЛАСОВАНО:

Заведующий выпускающей кафедрой АЭМИС

к.т.н. доцент Л.Ю. Вадова

Начальник ОУМБО И.В. Старикова

Рабочая программа зарегистрирована в ОУМБО: 09.04.02 - 12

СОДЕРЖАНИЕ

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1 Цель освоения дисциплины

Целью освоения дисциплины является развитие компетенций в области разработки и анализа объектов информационной безопасности, основанное на изучении математического аппарата.

1.2 Задачи освоения дисциплины (модуля)

Дисциплина «Математические основы криптологии» способствует подготовке студентов к решению следующих профессиональных задач:

1. Исследование математических зависимостей, лежащих в основе криптографических алгоритмов.
2. Проведение анализа уязвимости систем защиты информации путем исследования математических основ криптографических алгоритмов, на которых они построены.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Учебная дисциплина «Математические основы криптологии» Б1.В.ОД.1 включена в обязательный перечень дисциплин вариативной части (формируемой участниками образовательных отношений), определяющий направленность образовательной. Дисциплина реализуется в соответствии с требованиями ФГОС, ОП ВО и УП, по данному направлению подготовки.

Дисциплина базируется на дисциплинах математического блок апрограммы бакалавриата по направлению «Информационные системы и технологии».

Дисциплина «Математические основы криптологии» является основополагающей для изучения следующих дисциплин: «Моделирование систем информационной безопасности», такжепрактики: учебная (ознакомительная).

Рабочая программа дисциплины «Математические основы криптологии» для инвалидов и лиц с ограниченными возможностями здоровья разрабатывается индивидуально с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся, по их личному заявлению.

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

Дисциплина «Математические основы криптологии» формирует компетенцию ПКС-2 совместно с дисциплинами и практиками, указанными в таблице 1.
Дисциплинарная часть компетенции ПКС-3 «Способен проводить разработку и анализ объектов информационной безопасности»: способен понимать и применять на практике математические методы, на которых базируются алгоритмы, обеспечивающие информационную безопасность объектов.

Таблица 1- Формирование компетенций дисциплинами учебного плана

Наименование дисциплин, формирующих компетенцию совместно	Семестры, формирования дисциплины Компетенции берутся из Учебного плана по направлению подготовки бакалавра /специалиста/магистра»			
	1	*2*	*3*	*4*
ПКС-2 Способен проводить разработку и анализ объектов информационной безопасности				
Математические основы криптологии				
Организационно-правовые основы информационной безопасности				
Интеллектуальные методы в информационной безопасности				
Компьютерная вирусология				
Моделирование систем информационной безопасности				
Технологии центров обработки данных				
Программирование на языках низкого уровня в задачах защиты информации				
Программно-аппаратная защита информации				
Управление информационной безопасностью				
Стеганографические методы защиты информации				
Алгоритмы цифровой обработки ЦСП в системах управления				
Ознакомительная				
Практика по получению профессиональных умений и опыта научно-исследовательской деятельности				
Научно-исследовательская работа				
Преддипломная				
Выполнение и защита ВКР				

Таблица 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-2. Способен проводить разработку и анализ объектов информационной безопасности	ИПКС-2.1. Разрабатывает объекты информационной безопасности	***Знать:*** математический аппарат, описывающий взаимодействие информационных процессов в криптосистемах, математический аппарат, лежащий в основе алгоритмов шифрования, математический аппарат, лежащий в основе алгоритмов генерации псевдослучайных последовательностей	***Уметь:*** осуществлять математическую постановку задач в области криптологии; использовать математический аппарат при построении алгоритмов создания криптосистем, самостоятельно изучать криптографические алгоритмы и применять для решения задач факторизации чисел, проверки простоты чисел и др.	***Владеть:*** математическим аппаратом для решения нестандартных задач в области криптологии.	Выполнение сквозного индивидуального задания – портфолио, 17 задач	Вопросы для устного собеседования – 20 вопросов

Освоение дисциплины причастно к ТФ С/02.7, С/03.7 (ПС 06.032 «Специалист по безопасности компьютерных систем и сетей»), решает задачу исследования принципов функционирования средств и методов криптографической защиты информации.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Распределение трудоѐмкости дисциплины по видам работпо семестрам

Общая трудоѐмкость дисциплины составляет 4зач.ед. 144 часа, распределение часов по видам работ семестрам представлено в таблице 3.

Таблица 3 - Распределение трудоѐмкости дисциплины по видам работ по семестрамдля студентов очного обучения.

Вид учебной работы	**Трудоѐмкость в час**	
	Всего час.	**В т.ч. по семестрам**
		1 сем
Формат изучения дисциплины	с использованием элементов электронного обучения	
Общая трудоѐмкость дисциплины по учебному плану	**144**	**144**
1. Контактная работа:	**56**	**56**
1.1 Аудиторная работа, в том числе:	**51**	**51**
занятия лекционного типа (Л)	17	17
занятия семинарского типа (ПЗ-семинары, практ. Занятия и др)	34	34
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)	**88**	**88**
реферат/эссе (подготовка)		
расчѐтно-графическая работа (РГР) (подготовка)		
контрольная работа	40	40
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.)	30	30
Подготовка к зачѐту/ зачѐту с оценкой	18	18

4.2 Содержание дисциплины, структурированное по темам

Таблица 4 -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					
1 семестр										
Раздел 1. Арифметические основы криптологии										
ПКС-2 - ИПКС-2.1	**Тема 1.1.** НОД, НОК, простые числа. Варианты алгоритма Эвклида.	1		2		2	Подготовка к лекциям [6.1.1, 6.1.2], работа над сквозным индивидуальным заданием	Метод портфолио		
	Тема 1.2. Сравнения. Классы вычетов. Первообразные корни.	2		2		3	Подготовка к лекциям [6.1.1, 6.1.2], работа над сквозным индивидуальным заданием	Метод портфолио		
	Тема 1.3. Системы сравнений. Китайский алгоритм остатков.	2		2		5	Подготовка к лекциям [6.1.1, 6.1.2], работа над сквозным индивидуальным заданием	Метод портфолио		
	Тема 1.4. Дискретный логарифм. Символы Лежандра и Якоби.	2		4		5	Подготовка к лекциям [6.1.1, 6.1.2], работа над сквозным индивидуальным заданием	Метод портфолио		
	Тема 1.5. Использование арифметических алгоритмов в криптографии			4		10	Самостоятельное изучение разделов[6.1.3]. Работа над докладом по теме.			
	Итого по 1 разделу	**7**		**14**	**1**	**25**				
Раздел 2. Алгебраические основы криптологии										
ПКС-2 - ИПКС-2.1	**Тема 2.1.** Группы. Порядки элементов в группе. Подруппы. Смежные классы.	2		4		4	Подготовка к лекциям [6.1.5 - 6.1.7], работа над сквозным индивидуальным заданием	Метод портфолио		

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 2.2. Кольца и поля. Многочлены над полем. Неприводимые многочлены.	1		4		4	Подготовка к лекциям [6.1.5 - 6.1.7], работа над сквозным индивидуальным заданием	Метод портфолио		
	Тема 2.3. Конечное расширение поля. Алгебраическое замыкание поля.	1				2	Подготовка к лекциям [6.1.5 - 6.1.7], работа над сквозным индивидуальным заданием			
	Итого по 2 разделу	**4**		**8**	**1**	**10**				
Раздел 3. Эллиптические кривые										
ПКС-2 - ИПКС-2.1	**Тема 3.1.** Эллиптические кривые над полем вещественных чисел.	1		2		4	Подготовка к лекциям [6.1.5 - 6.1.7], работа над сквозным индивидуальным заданием			
	Тема 3.2. Эллиптические кривые над конечными полями.	2		4		6	Подготовка к лекциям [6.1.5, 6.1.7], работа над сквозным индивидуальным заданием	Метод портфолио		
	Тема 3.3. Использование эллиптических кривых в криптографических алгоритмах.	1		2		10	Самостоятельное изучение разделов[6.1.4]. Работа над докладом по теме.			
	Итого по 3 разделу	**4**		**8**	**1**	**20**				
Раздел 4. Псевдослучайные последовательности										
ПКС-2 - ИПКС-2.1	**Тема 4.1.** Понятие случайных и псевдослучайных последовательностей.Тестирование последовательностей	1				3	Подготовка к лекциям [6.1.5 - 6.1.7], работа над сквозным индивидуальным заданием	Метод портфолио		
	Тема 4.2. Алгоритмы генерации псевдослучайных после-	1		4		12	Самостоятельное изучение разделов[6.1.4]. Работа над докладом по			

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					
	довательностей						теме.			
	Итого по 4 разделу	**2**		**4**	**1**	**15**				
	Подготовка к зачѐту с оценкой				**1**	**18**				
	Итого за семестр	**17**		**34**	**5**	**88**				

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 текущей и промежуточной аттестации.

1. Примерная тематика заданий портфолио:

– нахождение НОД по алгоритму Эвклида;
– линейное разложение НОД по расширенному алгоритму Эвклида;
– поиск простых чисел до числа n (с помощью алгоритмов, представленных докладами);
– задать многочлены над полем GF_2;
– найти НОД многочленов и его линейное разложение;
– задать неприводимый многочлен $g(x)$ над полем GF_2 и сформировать поле многочленов $F[X]/g(x)$ как конечное расширение поля GF_2;
– построить таблицы Кэли для аддиттивной и мультипликативной групп полямногочленов $F[X]/g(x)$;
– построить эллиптическую кривую над полем характеристики $p>3$ (p-простое);
– найти порядок точки на эллиптической кривой.

2. Примерная тематика докладов:

– Решето Сундарама для поиска простых чисел
– Критерий простоты Вильсона
– Тест на простоту на основе малой теоремы Ферма, псевдопростые числа - числа Кармайк-ла
– Решето Аткина для поиска простых чисел
– Тест на простоту Миллера-Рабина
– ЭЦП на эллиптической кривой
– Квадратичный конгруэнтный генератор ПСП
– Генератор Эйхенауэра - Лена с обращением
– Генераторы Фибоначчи

3. Задания для самостоятельного решения и текущего контроля:

1) Найти вычет $a^{52782} (\mathrm{mod}\ m)$
2) Решить степенное сравнение $x^a \equiv q (\mathrm{mod}\ p)$
3) Найти символ Лежандра $\left(\frac{m}{q}\right)$
4) Найти порядок элемента ($\mathrm{ord}a$) в мультипликативной группе Z_p^* (для любых двух a)
5) Создать эллиптическую кривую:$E_p(a, b= a^{-1} (\mathrm{mod} p))$

Варианты (пример):

№ вар.	a=	p=	m=	q=
1	a=2	p=13	m=429	q=449
2	a=3	p=17	m=385	q=401
3	a=5	p=19	m=182	q=199

4	a=7	p=23	m=255	q=443
5	a=2	p=23	m=195	q=197

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 может применяться **балльно-рейтинговая/традиционная** система контроля и оценки успеваемости студентов.

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

Таблица 5

Шкала оценивания	**Оценка**
90-100	Отлично
75-90	Хорошо
55-74	Удовлетворительно
0-54	Неудовлетворительно

Таблица 6–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-2. Способен проводить разработку и анализ объектов информационной безопасности	ИПКС-2.1. Разрабатывает объекты информационной безопасности	Изложение учебного материала бессистемное, неполное, не способен использовать математический аппарат при построении алгоритмов создания криптосистем.	Фрагментарные, поверхностные знания математического аппарата; фрагментальное использование математических закономерностей для решения отдельных задач, неспособность создавать алгоритмы криптографии.	Знает математический аппарат, лежащий в основе алгоритмов криптографии; применяет на практике математический аппарат при построении алгоритмов создания криптосистем; испытывает затруднения при самостоятельном изучении криптографических алгоритмов.	Имеет глубокие системные знанияматематического аппарата, лежащего в основе алгоритмов криптографии; применяет на практике математический аппарат при построении алгоритмов создания криптосистем; при самостоятельном изучении криптографических алгоритмов проявляет инициативу, способен делать обоснованные выводы, проводить анализ результатов работы.

Таблица 7 - Критерии оценивания

Оценка	Критерии оценивания
Высокиий 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

6.1.3. Введение в теоретико-числовые методы криптографии : Учеб.пособие / М. М. Глухов [и др.]. - СПб.; М.; Краснодар : Лань, 2011. - 400 с.

6.1.4. Герман О.Н. Теоретико-числовые методы в криптографии : Учебник / О. Н. Герман, Ю. В. Нестеренко. - М. : Изд.центр "Академия", 2012. - 272 с.

6.2 Справочно-библиографическая литература

— *учебники и учебные пособия*

6.1.5. 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

6.1.6. 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

6.1.7. 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 Методические указания, рекомендации и другие материалы к занятиям

6.1.8. Метод. указания по организации аудиторной работы по дисциплине «Математические основы криптологии» для студентов направления подготовки09.04.02

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

6.1.9. Метод. указания по организации самостоятельной работы по дисциплине «Математические основы криптологии» для студентов направления подготовки

09.04.02 «Информационные системы и технологии» дневной формы обучения / НГТУ; Сост.: О.П. Тимофеева, Н.Новгород, 2020, 15 с.

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

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 8 -Перечень электронных библиотечных систем

№	Наименование ЭБС	Ссылка к ЭБС
1	Консультант студента	http://www.studentlibrary.ru/
2	Лань	https://e.lanbook.com/

7.2 Перечень свободно распространяемого программного обеспечения

Таблица 9 – Программное обеспечение, используемое студентами очного обучения

№ п/п	Программное обеспечение, используемое в университете на договорной основе	Программное обеспечение свободного распространения
1	MicrosoftWindows 10 (подпискаMSDN 700593597, подпискаDreamSparkPremium, 19.06.19)	Adobe Acrobat Reader https://acrobat.adobe.com/ru/ru/acrobat/pdf-reader.html
2	Microsoft VISUAL STUDIO 2008 (подписка MSDN 700593597, подпискаDreamSparkPremium, 19.06.19)	Visual Studio Code https://code.visualstudio.com/download
3	Microsoft office 2010 (Лицензия № 49487295 от 19.12.2011)	OpenOfficehttps://www.openoffice.org/ru/
4	КонсультантПлюс	PTC Mathcad Express https://www.mathcad.com/ru

7.3 Перечень современных профессиональных баз данных и информационных справочных систем

В таблице 10 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.

Таблица 10 - Перечень современных профессиональных баз данных и информационных справочных систем

№ п/п	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.gost.ru/portal/gost //home/standarts
2	Перечень профессиональных баз данных и информационных справочных систем	https://cyberpedia.su/21x47c0.html

3	Инструменты и веб-ресурсы для веб-разработки – 100+	https://techblog.sdstudio.top/blog/instrumenty-i-veb-resursy-dlia-veb-razrabotki-100-plus
4	Справочная правовая система «КонсультантПлюс»	доступ из локальной сети

8. ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОВЗ

В таблице 11 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 ДПИ НГТУ «Сведения об образовательной организации» https://dpi.nntu.ru/sveden/ovz/

Таблица 11 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

Согласно Федеральному Закону об образовании 273-ФЗ от 29.12.2012 г. ст. 79, п.8 "Профессиональное обучение и профессиональное образование обучающихся с ограниченными возможностями здоровья осуществляются на основе образовательных программ, адаптированных при необходимости для обучения указанных обучающихся". АОП разрабатывается по каждой направленности при наличии заявлений от обучающихся, являющихся инвалидами или лицами с ОВЗ и изъявивших желание об обучении по данному типу образовательных программ.

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 12 перечислены:

- учебные аудитории для проведения учебных занятий, оснащенные оборудованием и техническими средствами обучения;
- помещения для самостоятельной работы обучающихся, которые должны быть оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду ДПИ НГТУ.

Таблица 12 - Оснащенность аудиторий и помещений для самостоятельной работы обучающихся 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	**1161**Аудитория для	Комплект демонстрационного	• Microsoft Windows 7 (подписка

№	Наименование аудиторий и помещений для самостоятельной работы	Оснащенность аудиторий помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
	лекционных занятий Нижегородская обл., г. Дзержинск, ул. Гайдара, д. 49	оборудования: ПК, с выходом на мультимедийный проектор, на базе IntelPentium G4560 3.5 Ггц, 4 Гб ОЗУ, монитор 20’ – 1шт. Мультимедийный проектор Epson- 1 шт; Экран – 1 шт.	DreamSpark Premium) • Apache OpenOffice 4.1.8(свободное ПО); • Mozilla Firefox(свободное ПО); • Adobe Acrobat Reader (свободное ПО); 7-zip для Windows (свободное ПО);
2	**1329**Аудитория учебная аудитория для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Комплект демонстрационного оборудования: ПК, с выходом на мультимедийный проектор, на базе IntelPentium G4560 3.5 Ггц, 4 Гб ОЗУ, монитор 20’ – 1шт. Мультимедийный проектор Epson- 1 шт; Экран – 1 шт.	• Microsoft Windows 7 (подпискаDreamSpark Premium) • Apache OpenOffice 4.1.8(свободное ПО); • Mozilla Firefox(свободное ПО); • Adobe Acrobat Reader (свободное ПО); 7-zip для Windows (свободное ПО);
3	1234 Научно-техническая библиотека ДПИ НГТУ, студенческий читальный зал; Нижегородская обл., г. Дзержинск, ул. Гайдара, д. 49	Комплект демонстрационного оборудования: • ПК, с выходом на мультимедийный проектор, на базе IntelPentium G45603.5Ггц, 4 Гб ОЗУ, монитор 20’ – 1шт. • Мультимедийный проектор Epson- 1 шт; • Экран – 1 шт.; Набор учебно-наглядных пособий	• MicrosoftWindows 10 Домашняя (поставка с ПК) • LibreOffice 6.1.2.1. (свободное ПО) • FoxitReader (свободное ПО); • 7-zip для Windows (свободное ПО)
4	1443а компьютерный класс - помещение для СРС, курсового проектирования (выполнения курсовых работ), Нижегородская обл., г. Дзержинск, ул. Гайдара, д. 49	ПК на базе IntelCeleron 2.67 ГГц, 2 Гб ОЗУ, монитор Acer 17’ – 4 шт. ПК подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду университета	• Microsoft Windows 7 (подпискаDreamSpark Premium) • Apache OpenOffice 4.1.8(свободное ПО); • Mozilla Firefox(свободное ПО); • Adobe Acrobat Reader (свободное ПО); • 7-zip для Windows (свободное ПО); • КонсультантПлюс(ГПД № 0332100025418000079 от 21.12.2018);

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 «Математические основы криптологии», используются со-

временные 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 применяетсятрадиционная 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 (Таблица 4). Обозначаются ключевые аспекты тем, а также делаются акцен- ты 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 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 семинаров и 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 (семинарские) занятия обучающихся обеспечивают:

- проверку и уточнение знаний, полученных на лекциях;
- получение умений и навыков составления докладов и сообщений, обсуждения вопросов по учебному материалу дисциплины.

Приводятся конкретные методические указания для обучающихся по выполнению заданий портфолио, и по подготовке докладов; предъявляются требования к оформлению портфолио, к содержанию и представлению докладов.

Примерная тематика докладов:

1. Решето Сундарама для поиска простых чисел
2. Критерий простоты Вильсона
3. Тест на простоту на основе малой теоремы Ферма, псевдопростые числа - числа Кармайкла
4. Решето Аткина для поиска простых чисел
5. Тест на простоту Миллера-Рабина
6. Тест ан простоту Соловея-Штрассена
7. Теорема Поклингтона для построения простых чисел
8. Теорема Диемитко для построения простых чисел
9. Метод Маурера для построения простых чисел
10. Метод Михалеску для построения простых чисел
11. Факторизация методом пробных делений
12. Факторизация числа методом Полларда
13. Факторизация Ферма
14. Алгоритм факторизации Диксона
15. Алгоритм факторизации Бриллхарта-Моррисона
16. Метод квадратичного решета в решении задачи факторизации
17. Задача генерации случайной эллиптической кривой и выбор точки на ней
18. Шифрование и расшифрование текста на эллиптической кривой
19. ЭЦП на эллиптической кривой
20. Квадратичный конгруэнтный генератор ПСП
21. Генератор Эйхенауэра - Лена с обращением
22. Генераторы Фибоначчи
23. Генератор ANSI X9.17
24. Генератор FIPS - 186
25. Генератор Yarrow – 160
26. Принцип работы криптосистемы RSA
27. Алгоритм обмена ключами DH
28. Стандарт ЭЦП DSS
29. Схема ЭЦП Эль-Гамаля
30. Схема ЭЦП Рабина

10.5 Методические указания по выполнению контрольной работы

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 вРазделе 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 текущего контроля успеваемости

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

- выполнение заданий портфолио;
- подготовка доклада и выступление в сопровождении мультимедийной презентации.

11.1.1. Типовые задания для практических занятий

Типовые задания для практических занятий приведены в учебно-методических указаниях по организации 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 1 семестре обучения

Типовые вопросы для промежуточной аттестации в форме зачета с оценкой

1. Поиск простых чисел до числа n (рассказать об одном из алгоритмов)
2. Каноническое разложение числа на простые множители (рассказать об одном из алгоритмов)
3. Понятие вычета, классов вычетов, полной системы вычетов по модулю m, приведенной системы вычетов по модулю m
4. Понятие функции Эйлера для m
5. Понятие обратного элемента в Zm
6. Принципы решения сравнений (для простого и составного m)
7. Китайская теорема об остатках
8. Понятие первообразного корня (образующего элемента), его нахождение и формирование с его помощью приведенной системы вычетов
9. Понятие индекса числа. Смысл дискретного логарифма.
10. Принципы решения степенного (показательного) сравнения.
11. Понятие символа Лежандра и символа Якоби, алгоритмы их нахождения
12. Дать определение группы, абелевой группы, привести примеры.
13. Что такое порядок элемента в группе? (рассмотреть группы по сложению и умножению)
14. Какая группа называется циклической?
15. Как произвести разложение группы на подгруппы? (рассмотреть группы по сложению и умножению)
16. Как формируются смежные классы для подгруппы? (рассмотреть группы по сложению и умножению)
17. Дать определение кольца, привести примеры
18. Дать определение поля, поля Галуа. Привести примеры
19. Что такое область целостности?
20. Как задать многочлен над полем?
21. Что такое неприводимый многочлен над полем?
22. Что такое характеристика поля?

23. Нахождение НОД многочленов над полем F
24. Что такое расширение поля?
25. Что такое конечное расширение поля?
26. Что такое поле разложения многочлена?
27. Дать определение алгебраической кривой над полем.
28. Дать определение эллиптической кривой над полем.
29. Пояснить смысл бесконечно удаленной точки.
30. Пояснить смысл дискриминанта и j-инварианта эллиптической кривой.
31. Пояснить арифметические действия над точками эллиптической кривой, определенной над полем вещественных чисел.
32. Пояснить алгоритм получения точек эллиптической кривой над конечным полем.
33. Пояснить арифметические действия над точками эллиптической кривой, определенной над конечным полем.
34. Что такое порядок эллиптической кривой?
35. Что такое порядок точки на эллиптической кривой?
36. Что такое скалярно-кратные точки эллиптической кривой?
37. В чем состоит задача дискретного логарифмирования на эллиптических кривых?
38. Определение псевдослучайной последовательности, генератора ПСП.
39. Что такое линейный конгруэнтный генератор?
40. Что такое мультипликативный конгруэнтный генератор?

В полном объеме оценочные средства имеются на кафедре «АЭМИС». Оценочные средства могут быть получены по требованию.