Министерство науки и высшего образования Республики Казахстан

ВКТУ им.Д.Серикбаева

УТВЕРЖДАЮ:
Декан МШИ:
Оналбаева Ж.С.
_____2026 г.

ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ В КРИПТОГРАФИИ

Рабочая учебная программа (силлабус)

Образовательная программа: 6B06103 Математическое и компьютерное моделирование
Код дисциплины: TChMK4208
Количество кредитов: 5
Цикл: БД
Компонент: ВК

Усть-Каменогорск, 2026

Рабочая учебная программа (силлабус) разработана на «МШИ» на основании Государственных общеобязательных стандартов высшего и послевузовского образования (Приказ Министра науки и высшего образования РК №2 от 20.07.2022 г.), Правил организации учебного процесса по кредитной технологии обучения (Приказ Министра образования и науки РК от №152 от 20.04.2011 г.), Образовательной программы, Рабочего учебного плана, Каталога элективных дисциплин.

Одобрено Комиссией по обеспечению качества

Председатель — Мухамедова Р.О.
Дата 26.08.2026 г. протокол №1

Руководитель образовательной программы — Тезекпаева Ш.Т.
6В06103

Сотрудник библиотеки — Дроздова О.Н.

Разработал — Тураров А.К.
Старший преподаватель

СОГЛАСОВАНО:
Декан ШЦТиИИ — Хасенова З.Т.

1 ХАРАКТЕРИСТИКА ДИСЦИПЛИНЫ, ЕЕ МЕСТО В УЧЕБНОМ ПРОЦЕССЕ

1.1 Краткое описание дисциплины

Дисциплина является одной из основной профилирующей составляющей в подготовке специалистов в области защиты информации. В рамках дисциплины рассматриваются вопросы о теоретико-числовых принципах построения криптографических систем с симметричным и асимметричным ключом, математических методах расчета надежности, устойчивости криптографических систем, методах построения математических моделей защищаемой информации, шифров, криптографических систем и криптографических протоколов.

1.2 Цель и задачи изучения дисциплины

Цель изучения дисциплины:

изучение математических основ криптографии, математических методов построения криптографических систем, шифров и протоколов и методы расчета их надежности (криптостойкости).

Задачи изучения дисциплины:

- четкое осознание необходимости и важности математической подготовки для конкурентоспособного специалиста;
- ознакомление с основами классической и современной теории чисел, имеющими практические приложения к решению некоторых задачах профессиональной сферы;
- ознакомление обучающихся с математическими методами расчета надежности криптографических систем.

1.3 Цели устойчивого развития

Цель 3. Обеспечение здорового образа жизни и содействие благополучию для всех в любом возрасте

Цель 4. Обеспечение всеохватного и справедливого качественного образования и поощрение возможности обучения на протяжении всей жизни для всех

1.4 Результаты обучения

Результаты обучения определяются на основе Дублинских дескрипторов соответствующего уровня образования и выражаются через компетенции.

Формируемые ключевые компетенции	Результаты обучения (единицы ключевых компетенций)	
	образовательной программы	дисциплины
	РО11 - Проводить лабораторные и численные эксперименты, оценивать точность и корректность результатов моделирования при создании и программной реализации систем искусственного интеллекта	- основные свойства сравнений по модулю, алгоритмы проверки чисел на простоту и построения больших простых чисел; построение конечных полей; основные свойства групп и колец - применение расширенного алгоритма Евклида для быстрого нахождения НОД (целых чисел и многочленов) и обратных элементов в кольцах вычетов; решение линейных сравнений и уравнений в поле Галуа и в группе подстановок; определение разрешимости квадратичных сравнений - логически верно, аргументировано и ясно строить устную и письменную речь на языке обучения, грамотно применяя термины дисциплины - готовить и редактировать тексты профессионального назначения, публично представлять собственные и известные научные результаты, вести дискуссии. - иметь навыки применения и разработки эффективных алгоритмов для решения прикладных задач; быть готовыми к применению в профессиональной деятельности работе математических методов и средств
КК6 - Способность обеспечивать информационную безопасность на основе применения компьютерных систем и средств обработки, хранения и передачи информации и математического моделирования процессов, возникающих при защите информации	РО12 - Анализировать защиту информации объектов, систем, процессов с целью поиска эффективных и рациональных способов решения задач, уметь идентифицировать и устранять уязвимости, разрабатывать и применять методы защиты информации, а также анализировать и внедрять современные подходы для обеспечения безопасности компьютерных систем	

1.5 Образовательные технологии, применяемые при освоении дисциплины

1.5.1 Современные образовательные технологии

При проведении учебных занятий предусматривается использование следующих образовательных технологий:

- - лекции и онлайн-лекции, практические занятия с применением слайдов и других средств мультимедиа.

1.5.2 Адаптивные образовательные технологии (инклюзивное обучение)

Для успешного освоения дисциплины при обучении лиц с ограниченными возможностями здоровья могут применяться следующие адаптивные образовательные технологии:

- - предоставление электронных учебных пособий, ссылки на интернет ресурсы с материалами; - аудио- или видеозаписи лекций и лабораторных занятий; - предусмотрена возможность сдачи работ через портал СДО.

1.6 Пререквизиты

- Дискретная математика

1.7 Постреквизиты

1.8 Трудоемкость дисциплины

Виды работ	часы
Лекции	15
Практические работы	30
СРОП	30
СРО	75
Форма проведения итогового контроля	экзамен

2 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1 Тематический план

№	Наименование темы и её содержание	Часы	Результаты CDIO	Метод обучения	Литература
	Лекционные занятия				
1	**Тема 1. Криптография и делимость целых чисел.** Математическая модель шифрования. Симметричные и асимметричные криптосистемы. Свойства делимости. Теорема о делении с остатком, в том числе для отрицательных делимых.	1	Оценка и качественный анализ	теоретическое обучение	[4–5, 8, 10, 12, 16–17]
2	**Тема 2. НОД, НОК и алгоритм Евклида.** Связь НОД и НОК. Алгоритм Евклида и тождество Безу. Расширенный алгоритм Евклида. Теорема Ламе и оценка числа делений.	1	Оценка и качественный анализ	теоретическое обучение	[1–3, 10–11, 13]
3	**Тема 3. Простые числа и разложение на множители.** Простые, составные и взаимно простые числа. Теорема Евклида о бесконечности простых чисел. Основная теорема арифметики. Решето Эратосфена и граница пробных делений.	1	Оценка и качественный анализ	теоретическое обучение	[1–3, 9–11, 17]
4	**Тема 4. Взаимная простота и арифметические функции.** Критерий взаимной простоты и его следствия. Попарная взаимная простота. Мультипликативные функции, функция Эйлера и её вычисление. Целая и дробная части числа.	1	Оценка и качественный анализ	теоретическое обучение	[1–3, 10, 13]
5	**Тема 5. Сравнения и классы вычетов.** Сравнения целых чисел по модулю. Свойства сравнений, условия сокращения и перехода к другому модулю. Классы вычетов и полная система вычетов.	1	Оценка и качественный анализ	теоретическое обучение	[1–3, 10, 13]

№	Наименование темы и её содержание	Часы	Результаты CDIO	Метод обучения	Литература
6	**Тема 6. Кольцо вычетов и обратимые элементы.** Сложение и умножение классов вычетов. Обратимые элементы и делители нуля. Критерий обратимости. Вычисление обратного элемента расширенным алгоритмом Евклида.	1	Оценка и качественный анализ	теоретическое обучение	[1–3, 10, 13–14]
7	**Тема 7. Теоремы Ферма и Эйлера.** Малая теорема Ферма и теорема Эйлера. Вычисление обратных элементов и степеней по модулю. Условия корректного уменьшения показателя степени. Учебный пример RSA.	1	Оценка и качественный анализ	теоретическое обучение	[1–3, 10, 12–13]
8	**Тема 8. Подстановки и конечные группы.** Композиция подстановок, разложение на циклы, чётность и порядок. Подгруппы, циклические группы. Теорема Лагранжа. Симметрии правильного треугольника.	1	Оценка и качественный анализ	теоретическое обучение	[10, 13]
9	**Тема 9. Неприводимые многочлены и конечные поля.** Многочлены над полем вычетов по простому модулю. Построение конечного поля с помощью неприводимого многочлена. Арифметика поля. Цикличность мультипликативной группы и дискретный логарифм.	1	Оценка и качественный анализ	теоретическое обучение	[10, 12–13, 15–16]
10	**Тема 10. Линейные сравнения и китайская теорема об остатках.** Условие разрешимости линейного сравнения и число решений. Системы сравнений. Китайская теорема об остатках. Совместность систем с модулями, не являющимися взаимно простыми.	1	Оценка и качественный анализ	теоретическое обучение	[1–3, 10, 13]
11	**Тема 11. Сравнения высших степеней и поднятие корней.** Сведение к модулям, равным степеням простых чисел. Поднятие корней многочлена, регулярный и вырожденный случаи. Восстановление решений по китайской теореме об остатках.	1	Оценка и качественный анализ	теоретическое обучение	[10, 13, 21]
12	**Тема 12. Символы Лежандра и Якоби.** Квадратичные вычеты. Критерий Эйлера, свойства символа Лежандра и квадратичный закон взаимности. Вычисление символа Якоби и ограничения его применения при составном модуле.	1	Оценка и качественный анализ	теоретическое обучение	[1–3, 10–11, 13, 22]

№	Наименование темы и её содержание	Часы	Результаты CDIO	Метод обучения	Литература
13	**Тема 13. Псевдослучайные последовательности над конечным полем.** Линейные рекуррентные последовательности и регистры сдвига с обратной связью. Период и примитивные многочлены. Предсказуемость линейных генераторов и требования к криптографическим генераторам.	1	Оценка и качественный анализ	теоретическое обучение	[12–14, 23, 33]
14	**Тема 14. Факторизация и дискретный логарифм.** Пробные деления, метод Ферма и ρ-метод Полларда. Проверка и генерация простых чисел. Порядок элемента, генератор группы и алгоритм «малый шаг — большой шаг».	1	Оценка и качественный анализ	теоретическое обучение	[11, 13–14, 16, 24]
15	**Тема 15. Числа Кармайкла и алгоритмы арифметики.** Псевдопростые числа и критерий Корсельта. Ограничения теста Ферма и тест Миллера—Рабина. Умножение столбиком и алгоритм Карацубы. Двоичное возведение в степень по модулю.	1	Оценка и качественный анализ	теоретическое обучение	[14, 18–20, 25]
ИТОГО		**15**			
Практические занятия					
1	**Тема 1. Делимость и деление с остатком.** Проверка свойств делимости. Нахождение частного и остатка для положительных и отрицательных чисел. Проверка тождества деления и диапазона остатка с помощью Python.	4	Оценка и качественный анализ	алгоритмизированное обучение	[1–3, 6–7, 10, 12, 17]
2	**Тема 2. Расширенный алгоритм Евклида.** Вычисление НОД и НОК. Построение таблицы шагов алгоритма. Нахождение коэффициентов Безу и обратных элементов. Реализация алгоритма и проверка результата.	4	Оценка и качественный анализ	алгоритмизированное обучение	[1–3, 10–11, 13]
3	**Тема 3. Простые числа и решето Эратосфена.** Пробные деления и решето Эратосфена. Разложение целых чисел на простые множители. Проверка полноты разложения и сравнение числа операций.	4	Оценка и качественный анализ	алгоритмизированное обучение	[1–3, 10–11, 13]

№	Наименование темы и её содержание	Часы	Результаты CDIO	Метод обучения	Литература
4	**Тема 4. Сравнения и классы вычетов.** Построение систем вычетов. Проверка и преобразование сравнений. Сокращение сравнений с учётом НОД. Работа с отрицательными представителями классов вычетов.	4	Оценка и качественный анализ	алгоритмизированное обучение	[1–3, 10, 13]
5	**Тема 5. Кольцо вычетов и обратные элементы.** Таблицы сложения и умножения. Поиск обратимых элементов и делителей нуля. Вычисление обратного элемента и проверка произведения по модулю.	4	Оценка и качественный анализ	алгоритмизированное обучение	[1–3, 10, 13]
6	**Тема 6. Вычисление функции Эйлера.** Подсчёт взаимно простых остатков. Вычисление функции Эйлера по разложению числа. Проверка мультипликативности и сравнение способов вычисления.	4	Оценка и качественный анализ	алгоритмизированное обучение	[1–3, 10, 13]
7	**Тема 7. Подстановки и группы.** Композиция и обратная подстановка, разложение на циклы. Вычисление знака и порядка. Подгруппы и симметрии правильного треугольника. Проверка результатов.	4	Оценка и качественный анализ	алгоритмизированное обучение	[10, 13]
8	**Тема 8. Построение конечных полей.** Проверка неприводимости многочлена малой степени. Арифметика построенного поля, таблицы операций и обратные элементы. Решение линейных уравнений над конечным полем.	3	Оценка и качественный анализ	алгоритмизированное обучение	[10, 12–13]
ИТОГО		**30**			

2.2 Задания для самостоятельной работы обучающегося (СРО)

Тема	Содержание задания	Форма контроля	Срок сдачи, неделя	Трудоемкость в часах	Результаты CDIO

Тема	Содержание задания	Форма контроля	Срок сдачи, неделя	Трудоемкость в часах	Результаты CDIO
9. Линейные сравнения и китайская теорема об остатках. 10. Сравнения высших степеней и поднятие корней. 11. Символы Лежандра и Якоби.	Решение линейных сравнений и систем по КТО; поднятие корней по степеням простых чисел; вычисление символов Лежандра и Якоби и исследование разрешимости квадратных сравнений. Ручное решение, проверка в Python и оформление отчёта.	Защита работы	8	40	Оценка и качественный анализ
12. Квадратные корни по модулю. 13. Линейные регистры над конечным полем. 14. Факторизация, проверка простоты и дискретный логарифм. 15. Числа Кармайкла, умножение и возведение в степень.	Вычисление квадратных корней алгоритмом Тонелли — Шенкса; построение линейных регистров и анализ периода; факторизация, проверка простоты и вычисление дискретного логарифма; исследование чисел Кармайкла; умножение Карацубы и двоичное возведение в степень. Проверка в Python и оформление отчёта.	Защита работы	15	35	Оценка и качественный анализ
ИТОГО				**75**	

2.3 График сдачи заданий по дисциплине

Вид задания	Академический период обучения, неделя														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Знание															

Вид задания	Академический период обучения, неделя														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Практическая работа 1			+												
Практическая работа 2				+	+	+									
Практическая работа 3							+								
Практическая работа 4								+							
Практическая работа 5										+					
Практическая работа 6											+				
Практическая работа 7													+		
Практическая работа 8														+	
Понимание															
Практическая работа 1			+												
Практическая работа 2				+	+	+									
Практическая работа 3							+								
Практическая работа 4								+							
Практическая работа 5										+					
Практическая работа 6											+				
Практическая работа 7													+		
Практическая работа 8														+	
Применение															
Практическая работа 1			+												
Практическая работа 2				+	+	+									
Практическая работа 3							+								
Практическая работа 4								+							
Тест 1								+							
Практическая работа 5										+					

Вид задания	Академический период обучения, неделя														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Практическая работа 6											+				
Практическая работа 7													+		
Практическая работа 8														+	
Тест 2															+
Анализ															
Практическая работа 1			+												
Практическая работа 2				+	+	+									
Практическая работа 3							+								
Практическая работа 4								+							
Тест 1								+							
Практическая работа 5										+					
Практическая работа 6											+				
Практическая работа 7													+		
Практическая работа 8														+	
Тест 2															+

3 ОЦЕНКА ЗНАНИЙ ОБУЧАЮЩЕГОСЯ

Преподаватель проводит все виды работ текущего контроля и выводит соответствующую оценку текущей успеваемости обучающихся два раза в академический период. По результатам текущего контроля формируется рейтинг 1 и 2. Учебные достижения обучающегося оцениваются по 100-балльной шкале, итоговая оценка Р1 и Р2 выводится как средняя арифметическая из оценок текущей успеваемости. Оценка работы обучающегося в академическом периоде осуществляется преподавателем в соответствии с графиком сдачи заданий по дисциплине. Система контроля может сочетать письменные и устные, групповые и индивидуальные формы.

Период	Вид работы	Итоговая оценка
1-й рейтинг	Практическая работа 1	0-100
	Практическая работа 2	
	Практическая работа 3	
	Практическая работа 4	
	Тест 1	
2-й рейтинг	Практическая работа 5	0-100
	Практическая работа 6	
	Практическая работа 7	
	Практическая работа 8	
	Тест 2	
Итоговый контроль	экзамен	0-100

3.1 Политика оценивания результатов обучения по видам работ

Вид работы	**90-100**	**70-89**	**50-69**	**0-49**
	Отлично	**Хорошо**	**Удовлетворительно**	**Неудовлетворительно**
Работа на практических (семинарских) занятиях	выполнил практическую работу в полном объеме с соблюдением необходимой последовательности действий; в ответе правильно и аккуратно	выполнил требования к оценке «5», но допущены 2-3 недочета. Ответ обучающегося на вопросы удовлетворяет основным требованиям к ответу на 5, но	выполнил работу не полностью, но не менее 50% объема практической работы, что позволяет получить правильные результаты и выводы; в ходе	выполнил работу не полностью или объем выполненной части работ не позволяет сделать правильных выводов. При ответе на вопросы демонстрирует не

	выполняет все записи, таблицы, рисунки, чертежи, графики, вычисления; правильно выполняет анализ ошибок. При ответе на вопросы правильно понимает сущность вопроса, дает точное определение и истолкование основных понятий; сопровождает ответ новыми примерами, умеет применить знания в новой ситуации; может установить связь между изучаемым и ранее изученным материалом, а также с материалом, усвоенным при изучении других дисциплин.	дан без применения знаний в новой ситуации, без использования связей с ранее изученным материалом и материалом, усвоенным при изучении других дисциплин; допущены одна ошибка или не более двух недочетов, обучающийся может их исправить самостоятельно или с небольшой помощью преподавателя.	проведения работы были допущены ошибки. При ответе на вопросы обучающийся правильно понимает сущность вопроса, но в ответе имеются отдельные проблемы в усвоении вопросов курса, не препятствующие дальнейшему усвоению программного материала; допущено не более одной грубой ошибки и двух недочетов.	владение основными знаниями и умениями в соответствии с требованиями программы; допущены больше ошибок и недочетов, чем необходимо для оценки 3 или не может ответить ни на один из поставленных вопросов.

Итоговая оценка знаний обучающего по дисциплине осуществляется по 100 балльной системе и включает:
- 60% результатов текущей успеваемости;
- 40% результата, полученного на экзамене.

Формула подсчета итоговой оценки:

$$И = 0{,}6\frac{P_1+P_2}{2} + 0{,}4Э \quad (1)$$

где Р1, Р2 – цифровые эквиваленты оценок первого, второго рейтингов соответственно; Э – цифровой эквивалент оценки на экзамене.

Буквенная система оценки учебных достижений обучающихся, соответствующая цифровому эквиваленту по четырехбалльной системе:

Оценка по буквенной системе	Цифровой эквивалент	Баллы (%-ное содержание)	Оценка по традиционной системе
A	4.0	95-100	Отлично
A-	3.67	90-94	

Оценка по буквенной системе	Цифровой эквивалент	Баллы (%-ное содержание)	Оценка по традиционной системе
B+	3.33	85-89	Хорошо
B	3.0	80-84	
B-	2.67	75-79	
C+	2.33	70-74	
C	2.0	65-69	Удовлетворительно
C-	1.67	60-64	
D+	1.33	55-59	
D	1.0	50-54	
FX	0.5	25-49	Неудовлетворительно
F	0	0-24	

4 ПОЛИТИКА ДИСЦИПЛИНЫ

Обучающийся обязан:

-посещение лекционных и практических занятий по расписанию является обязательным; -присутствие студентов на занятиях проверяется в начале занятий. В случае опоздания студент должен бесшумно войти в аудиторию и включиться в работу, а в перерыве объяснить преподавателю причину опоздания; -два опоздания на занятия приравниваются к одному пропуску занятия; -оцениваемые в баллах работы следует сдавать в установленные сроки. За несвоевременную сдачу работ количество баллов снижается. Студенты, не сдавшие все задания, к экзамену не допускаются; -повторное прохождение студентом рубежного контроля, в случае получения неудовлетворительной оценки, не допускается; -студенты, получившие средний рейтинг Рср = (Р1 + Р2)/2 менее 50%, к экзамену не допускаются; -в течение занятий мобильные телефоны должны быть отключены; -студент обязан приходить на занятия в деловой одежде.

Инструменты искусственного интеллекта (ИИ) разрешается использовать только в качестве вспомогательного средства для поиска информации и уточнения идей. При использовании ИИ необходимо обязательно указать ссылку на использованный инструмент или источник. Полное выполнение задания с помощью ИИ, представление готового ответа без изменений, отсутствие ссылки или сокрытие факта использования ИИ считается нарушением требований академической честности.

5 СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

5.1 Основная литература

1. Виноградов, И. М. Основы теории чисел / И. М. Виноградов. — Москва: Наука, 2021. — 402 с.
2. Бухштаб, А. А. Теория чисел / А. А. Бухштаб. — Санкт-Петербург: Лань, 2020. — 384 с.
3. Осипов, Н. Н. Теория чисел / Н. Н. Осипов. — Красноярск: Издательство Сибирского федерального университета, 2008. — 117 с.
4. Фомичев, В. М. Дискретная математика и криптология / В. М. Фомичев. — Москва: Диалог МИФИ, 2003. — 400 с.
5. Романьков, В. А. Введение в криптографию: курс лекций / В. А. Романьков. — Москва: Форум, 2012. — 240 с.
6. Жданов, О. Н. Сборник задач по криптографическим методам защиты информации: учебное пособие / О. Н. Жданов, К. К. Елемесов. — Алматы: КазНТУ имени К. И. Сатпаева, 2014. — 73 с.
7. Кукина, Е. Г. Введение в криптографию. Сборник задач и упражнений / Е. Г. Кукина, В. А. Романьков. — Омск: Издательство ОмГУ, 2013.
8. Әбдіқалықов, Қ. Ә. Криптографияның негіздері : оқулық / Қ. Ә. Әбдіқалықов. — Алматы, 2012. — 184 бет.
9. Оразбаев, Б. М. Сандар теориясы / Б. М. Оразбаев. — Алматы: Мектеп, 1979. — 393 бет.
10. Мартынов, Л. М. Алгебра и теория чисел для криптографии: учебное пособие / Л. М. Мартынов. — Санкт-Петербург: Лань, 2020. — 456 с.

11. Панкратова, И. А. Теоретико-числовые методы криптографии : учебное пособие / И. А. Панкратова. — Томск : Томский государственный университет, 2009. — 120 с.

12. Paar, C. Understanding Cryptography: A Textbook for Students and Practitioners / C. Paar, J. Pelzl. — Berlin ; Heidelberg: Springer, 2010. — DOI: 10.1007/978-3-642-04101-3.

13. Trappe, W. Introduction to Cryptography with Coding Theory / W. Trappe, L. C. Washington. — 2nd ed. — Pearson Education, 2006.

14. Katz, J. Introduction to Modern Cryptography / J. Katz, Y. Lindell. — 2nd ed. — CRC Press, 2015.

15. Zheng, Z. Modern Cryptography. Volume 1: A Classical Introduction to Informational and Mathematical Principle / Z. Zheng. — Singapore: Springer, 2022. — DOI: 10.1007/978-981-19-0920-7.

16. Boneh, D. A Graduate Course in Applied Cryptography / D. Boneh, V. Shoup. — Version 0.6, January 2023. — Текст: электронный. — URL: https://toc.cryptobook.us.

17. Kraft, J. S. An Introduction to Number Theory with Cryptography / J. S. Kraft, L. C. Washington. — 2nd ed. — CRC Press, 2018.

18. Эриксон, Дж. Алгоритмы / Дж. Эриксон ; перевод с английского А. В. Спастина, П. Б. Иванова. — Москва : ДМК Пресс, 2023. — 526 с.

19. Erickson, J. Algorithms / J. Erickson. — 1st ed. — 2019. — Текст: электронный. — URL: https://jeffe.cs.illinois.edu/teaching/algorithms.

20. Shoup, V. A Computational Introduction to Number Theory and Algebra / V. Shoup. — 2nd ed. — Cambridge University Press, 2008. — URL: https://www.shoup.net/ntb.

21. Conrad, K. Hensel’s Lemma: авторский конспект / K. Conrad. — Текст: электронный. — URL: https://kconrad.math.uconn.edu/blurbs/gradnumthy/hensel.pdf.

22. Hashing to Elliptic Curves / A. Faz-Hernandez, S. Scott, N. Sullivan, R. S. Wahby, C. A. Wood. — RFC 9380. — 2023. — DOI: 10.17487/RFC9380.

23. Recommendation for Random Bit Generator (RBG) Constructions / E. Barker, J. Kelsey, K. McKay, A. Roginsky, M. Sönmez Turan. — NIST SP 800-90C. — 2025. — DOI: 10.6028/NIST.SP.800-90C.

24. Digital Signature Standard (DSS) / National Institute of Standards and Technology. — FIPS 186-5. — 2023. — DOI: 10.6028/NIST.FIPS.186-5.

25. Agrawal, M. PRIMES is in P / M. Agrawal, N. Kayal, N. Saxena // Annals of Mathematics. — 2004. — Vol. 160, No. 2. — P. 781–793. — DOI: 10.4007/annals.2004.160.781. — Исправление: Errata: PRIMES is in P // Annals of Mathematics. — 2019. — Vol. 189, No. 1. — P. 317–318. — DOI: 10.4007/annals.2019.189.1.6.

5.2 Дополнительная литература

26. Нечаев, В. И. Элементы криптографии, основы теории защиты информации / В. И. Нечаев. — Москва: Высшая школа, 1999. — 172 с.

27. Гашков, С. Б. Арифметика. Алгоритмы. Сложность вычислений / С. Б. Гашков, В. Н. Чубариков. — Москва: Высшая школа. — 320 с.

28. Рожков, А. В. Теоретико-числовые методы в криптографии : учебное пособие / А. В. Рожков, О. В. Ниссенбаум. — Тюмень : Издательство ТюмГУ, 2007.

29. Рябко, Б. Я. Криптографические методы защиты информации / Б. Я. Рябко, А. Н. Фионов. — Москва: Горячая линия — Телеком, 2005. — 229 с.

30. IPR SMART: цифровой образовательный ресурс: сайт. — URL: http://www.iprbookshop.ru. — Текст: электронный.

31. ScienceDirect: электронная платформа научных публикаций: сайт. — URL: http://www.sciencedirect.com. — Текст: электронный.

32. EBSCO Discovery Service (EDS): электронная поисковая система: сайт. — URL: http://search.ebscohost.com. — Текст: электронный.

33. Paar, C. Understanding Cryptography: From Established Symmetric and Asymmetric Ciphers to Post-Quantum Algorithms / C. Paar, J. Pelzl, T. Güneysu. — 2nd ed. — Berlin; Heidelberg: Springer, 2024. — XXI, 543 p. — DOI: 10.1007/978-3-662-69007-9.