

**МИНОБРНАУКИ РОССИИ**  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ  
ВЫСШЕГО ОБРАЗОВАНИЯ  
**«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ  
ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В.Г.ШУХОВА»**  
(БГТУ им. В.Г. Шухова)

УТВЕРЖДАЮ  
Директор института энергетики,  
информационных технологий и  
управляющих систем  
Белоусов А.В.  
«\_\_\_\_\_» \_\_\_\_\_ 2021 г.



**РАБОЧАЯ ПРОГРАММА**  
дисциплины

**Математика криптографии**

направление подготовки:

10.05.03 Информационная безопасность автоматизированных систем

Специализация программы:

Безопасность открытых информационных систем

Квалификация

Специалист по защите информации

Форма обучения

очная

Институт энергетики, информационных технологий и управляющих систем

Кафедра Программного обеспечения вычислительной техники и  
автоматизированных систем

Рабочая программа составлена на основании требований:

- Федерального государственного образовательного стандарта высшего образования – специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем, утвержденного приказом Минобрнауки России от 26.11.2020 №1457
- учебного плана, утвержденного ученым советом БГТУ им. В.Г. Шухова в 2021 году.

Составитель: к.т.н., доцент  (Сергиенко Е.Н.)  
(ученая степень и звание, подпись) (инициалы, фамилия)

Рабочая программа обсуждена на заседании кафедры

« 14 » 05 2021 г., протокол № 8

Заведующий кафедрой: к.т.н., доцент  (Поляков В.М.)  
(ученая степень и звание, подпись) (инициалы, фамилия)


Рабочая программа согласована с выпускающей кафедрой программного обеспечения вычислительной техники и автоматизированных систем  
(наименование кафедры/кафедр)

Заведующий кафедрой: к.т.н., доцент  (Поляков В.М.)  
(ученая степень и звание, подпись) (инициалы, фамилия)

« 14 » 05 2021 г.

Рабочая программа одобрена методической комиссией института

« 20 » 05 2021 г., протокол № 9

Председатель к.т.н., доцент  (Семернин А.Н.)  
(ученая степень и звание, подпись) (инициалы, фамилия)

## 1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Категория (группа) компетенций	Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Наименование показателя оценивания результата обучения по дисциплине
Общепрофессиональные компетенции	ОПК-3. Способен использовать математические методы необходимые для решения задач профессиональной деятельности	ОПК-3.1 Осуществляет обоснованный выбор математических методов для решения типовых задач	<p><b>Знать:</b> Основные теоремы генерации конечного поля. Методы проверки числа на простоту, методы вычисления.</p> <p><b>Уметь:</b> Решать системы линейных однородных уравнений. Находить общее решение системы.</p> <p><b>Владеть:</b> Навыками применения расширенного алгоритма Евклида для многочленов над полем рациональных чисел; над конечным полем</p>
		ОПК-3.2 Решает типовые задачи математическими методами	<p><b>Знать:</b> Основные теоремы о базисе. Канонический базис.</p> <p><b>Уметь:</b> Находить базис системы векторов. Определять линейное подпространство. Его размерность.</p> <p><b>Владеть:</b> Навыками построения процесса ортогонализации Грамма-Шмидта</p>
	ОПК-10 Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.1 Анализирует криптографические методы, реализованные в средствах защиты информации	<p><b>Знать:</b> Теорема Поклингтона и ее применение для генерации простых чисел. Алгоритм Маурера генерации простых чисел.</p> <p><b>Уметь:</b> Применять полиномиальный тест. Тест Ферма. Псевдопростые числа. Числа Кармайкла. Тест «испытание квадратным корнем»</p> <p><b>Владеть:</b> Навыками применения алгоритм проверки чисел на простоту, алгоритма генерации простых чисел</p>

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

### 1. Компетенция ОПК-3. Способен использовать математические методы необходимые для решения задач профессиональной деятельности

Данная компетенция формируется следующими дисциплинами.

Стадия	Наименования дисциплины
1.	Математический анализ
2.	Алгебра и геометрия
3.	Дискретная математика
4.	Теория вероятностей и математическая статистика
5.	Математическая логика и теория алгоритмов
6.	Вычислительная математика
7.	Исследование операций
8.	Теория информации
9.	Математика криптографии
10.	Подготовка к процедуре защиты и защита выпускной квалификационной работы

### 2. Компетенция ОПК-10. Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности

Данная компетенция формируется следующими дисциплинами.

Стадия	Наименования дисциплины
1.	Методы и средства криптографической защиты информации
2.	Математика криптографии
3.	Криптографические интерфейсы
4.	Квантовые вычисления и квантовая криптография
5.	Подготовка к процедуре защиты и защита выпускной квалификационной работы

### 3. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 5 зач. единиц, 180 часов.

Форма промежуточной аттестации: экзамен.

Вид учебной работы	Всего часов	Семестр № 5
Общая трудоемкость дисциплины, час	180	180
<b>Контактная работа (аудиторные занятия), в т.ч.:</b>	90	90
лекции	34	34
лабораторные	17	17
практические	34	34
групповые консультации в период теоретического обучения и промежуточной аттестации	5	5
контроль самостоятельной работы	-	-
<b>Самостоятельная работа студентов, включая индивидуальные и групповые консультации, в том числе:</b>	90	90
Курсовой проект	-	-
Курсовая работа	-	-
Расчетно-графическое задания	-	-
Индивидуальное домашнее задание	-	-
Самостоятельная работа на подготовку к аудиторным занятиям (лекции, практические занятия, лабораторные занятия)	54	54
Экзамен	36	36

## 4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

### 4.1 Наименование тем, их содержание и объем

Курс 3 Семестр 5

№ п/п	Наименование раздела (краткое содержание)	Объем на тематический раздел по видам учебной нагрузки, час			
		Лекции	Практические занятия	Лабораторные занятия	Самостоятельная работа
1. Линейные пространства над конечным полем.					
	Линейные пространства над конечным полем. Базис и размерность. Порождающая матрица.	4	4	-	5
2. Расширенный алгоритм Евклида.					
	Расширенный алгоритм Евклида. Применение к многочленам над полем рациональных чисел и конечным полем.	6	6	3	10
3. Конечные поля (поля Галуа).					
	Конечные поля (поля Галуа). Расширение простого поля. Арифметика конечных полей. Нахождение обратного элемента поля.	6	4	4	8
4. Применение простых чисел в криптографии.					
	Применение простых чисел в криптографии. Проверка чисел на простоту. Алгоритмы генерации простых чисел.	4	4	4	8
5. Задача факторизации чисел.					
	Задача факторизации чисел. Алгоритмы факторизации.	4	6	2	8
6. Определение дискретного логарифма.					
	Определение дискретного логарифма. Количество значений дискретного логарифма элемента поля. Алгоритмы дискретного логарифмирования.	6	6	2	8
7. Определение ПСП.					
	Определение ПСП. Методы генерации ПСП. Применение ПСП в криптографии.	4	4	2	7
	<b>ВСЕГО</b>	<b>34</b>	<b>34</b>	<b>17</b>	<b>54</b>

### 4.2. Содержание практических (семинарских) занятий

№ п/п	Наименование раздела дисциплины	Тема практического занятия	К-во часов	К-во часов СРС
семестр № 5				
1	Линейные пространства над конечным полем	Линейные пространства	4	4
2	Расширенный алгоритм Евклида	Расширенный алгоритм Евклида в кольце чисел (кольце вычетов) Расширенный алгоритм Евклида в кольце многочленов над полем	6	4
3	Конечные поля (поля Галуа)	Структура конечного поля Генерация конечного поля	4	4

		Арифметика конечного поля		
4	Применение простых чисел в криптографии	Проверка числа на простоту. Генерация простых чисел.	4	4
5	Задача факторизации чисел	Факторизация чисел	6	4
	Определение дискретного логарифма	Вычисление дискретного логарифма	6	4
	Определение ПСП	Генератор RC4	4	4
ИТОГО:			34	28
ВСЕГО:				62

### 4.3. Содержание лабораторных занятий

№ п/п	Наименование раздела дисциплины	Тема лабораторного занятия	К-во часов	К-во часов СРС
семестр № 5				
1.	Линейные пространства над конечным полем		-	-
2.	Расширенный алгоритм Евклида	Алгоритм быстрого возведения в степень	8	4
		Расширенный алгоритм Евклида в кольце целых чисел. Линейное представление НОД двух целых чисел		
		Расширенный алгоритм Евклида в кольце $Z_n$ . Вычисление обратного элемента		
		Расширенный бинарный алгоритм Евклида. Другие формы алгоритма		
	Расширенный алгоритм Евклида для многочленов над полем рациональных чисел; над конечным полем			
3.	Конечные поля (поля Галуа)	Генерация конечного поля	6	3
		Определение порядка элемента поля		
		Арифметика конечного поля		
		Нахождение обратного элемента конечного поля		
4.	Применение простых чисел в криптографии	Алгоритм проверки чисел на простоту	8	3
		Алгоритм генерации простых чисел		
5.	Задача факторизации чисел	Факторизация чисел	8	4
6.	Определение дискретного логарифма	Вычисление дискретного логарифма	2	1
7.	Определение ПСП	Генератор RC4	2	1
ИТОГО:			17	16
ВСЕГО:				33

### 4.4. Содержание курсового проекта/работы

Не предусмотрено учебным планом

#### **4.5. Содержание расчетно-графического задания, индивидуальных домашних заданий**

Не предусмотрено учебным планом

### **5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ**

#### **5.1. Реализация компетенций**

##### **1. Компетенция ОПК-3. Способен использовать математические методы необходимые для решения задач профессиональной деятельности**

Наименование индикатора достижения компетенции	Используемые средства оценивания
ОПК-3.1 Осуществляет обоснованный выбор математических методов для решения типовых задач	устный опрос, защита лабораторной работы, экзамен
ОПК-3.2 Решает типовые задачи математическими методами	собеседование, защита лабораторной работы, экзамен

##### **2. Компетенция ОПК-10. Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности**

Наименование индикатора достижения компетенции	Используемые средства оценивания
ОПК-10.1 Анализирует криптографические методы, реализованные в средствах защиты информации	устный опрос, защита лабораторной работы, экзамен



## 5.2. Типовые контрольные задания для промежуточной аттестации

### 5.2.1. Перечень контрольных вопросов (типовых заданий) для экзамена

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
1.	Линейные пространства над конечным полем ОПК-3.1,3.2	<p>Определение линейного пространства (ЛП) над полем. Примеры линейных пространств</p> <p>Определение линейной комбинации векторов ЛП. Линейно зависимые и линейно независимые системы векторов</p> <p>Определение базиса и размерности ЛП. Разложение вектора по базису. Число базисных векторов и количество базисов в <math>L_n</math></p> <p>Выражение результатов линейных операций над векторами в базисе</p> <p>Основные теоремы о базисе. Канонический базис</p> <p>Переход от одного базиса к другому. Матрица перехода</p> <p>Нахождение базиса системы векторов</p> <p>Определение линейного подпространства. Его размерность. Примеры линейных подпространств</p> <p>Линейная оболочка системы векторов как подпространство. Его базис и размерность</p> <p>Изоморфизм линейных подпространств</p> <p>Решение системы линейных однородных уравнений. Общее решение системы</p> <p>Пространства со скалярным произведением. Геометрия пространства</p> <p>Ортогональные и ортонормированные системы векторов. Ортогональный и ортонормированный базис. Выражение скалярного произведения: в базисе; в ортонормированном базисе</p> <p>Процесс ортогонализации Грамма-Шмидта</p>
2.	Расширенный алгоритм Евклида ОПК-3.1,3.2	<p>Ортогональное дополнение к линейному подпространству евклидова пространства</p> <p>Линейное пространство над конечным полем <math>X</math>. Пространство <math>Q=X^n</math>; его размерность и мощность</p> <p>Подпространства пространства <math>Q</math>. Порождающая и проверочная матрицы. Их канонические формы</p> <p>Алгоритм быстрого возведения в степень</p> <p>Определение и свойства функции Эйлера</p> <p>Приведенная система вычетов</p> <p>Теорема Ферма и Эйлера. Их применение</p> <p>Различные формы расширенного алгоритма Евклида в кольце целых чисел</p> <p>Расширенный алгоритм Евклида в кольце <math>Z_n</math>. Вычисление обратного элемента</p> <p>Расширенный алгоритм Евклида для многочленов: над полем рациональных чисел; над конечным полем <math>Z_p</math></p>
3.	Конечные поля (поля Галуа) ОПК-3.1,3.2	<p>Общее определение конечного поля (поля Галуа). Простые поля.</p> <p>Алгебраические свойства конечных полей</p> <p>Определение примитивного элемента конечного поля. Теорема его существования</p> <p>Характер конечного поля. Числа поля. Степень суммы элементов поля</p>

		<p>Основная теорема теории конечных полей. Количество элементов поля.</p> <p>Расширение полей с помощью неприводимого многочлена</p> <p>Примитивный элемент и примитивный многочлен поля <math>GF(p^m)</math></p> <p>Структура конечного поля</p> <p>Арифметика конечного поля. Операция умножения. Процедура <math>xtime</math></p> <p>Структура полей: <math>GF(p^2)</math>; <math>GF(p^m)</math></p>
4.	<p>Применение простых чисел в криптографии</p> <p>ОПК-10.1</p>	<p>Количество простых чисел. Неравенство Чебышева. Числа Ферма. Числа Мерсенны.</p> <p>Детерминированные и вероятностные тесты проверки чисел на простоту</p> <p>Критерий Вильсона. Полиномиальный тест</p> <p>Тест Ферма. Псевдопростые числа. Числа Кармайкла</p> <p>Тест «испытание квадратным корнем»</p> <p>Различные варианты теста Миллера-Рабина</p> <p>Алгоритмы генерации простых чисел с заданной разрядностью</p> <p>Теорема Поклингтона и ее применение для генерации простых чисел</p> <p>Алгоритм Маурера генерации простых чисел</p>
5.	<p>Задача факторизации чисел</p> <p>ОПК-3.2</p>	<p>Задача факторизации чисел. Метод пробных делений</p> <p>Алгоритм вычисления <math>[\square n]</math></p> <p>Метод Ферма факторизации чисел</p> <p><math>\square</math> – метод Полларда факторизации чисел</p> <p><math>(\square-1)</math> – метод Полларда факторизации чисел</p>
6.	<p>Определение дискретного логарифма</p> <p>ОПК-3.2,10.1</p>	<p>Определение дискретного логарифма в циклической мультипликативной группе. Условие его существования. Случай неединственности.</p> <p><math>\rho</math> – метод Полларда вычисления дискретного логарифма</p> <p>Вычисление дискретного логарифма с помощью КТО (Метод Нечаева)</p> <p>Алгоритм «baby-step»</p> <p>Шифр Вернама</p>
7.	<p>Определение ПСП</p> <p>ОПК-10.1</p>	<p>Генераторы псевдослучайных чисел (ПСЧ)</p> <p>Алгоритм RC4</p> <p>Алгоритм RSA. Генератор ПСЧ на основе RSA</p> <p>Датчики M-последовательностей</p> <p>Тест «стопка книг»</p>

### 5.3. Типовые контрольные задания (материалы) для текущего контроля в семестре

*Текущий контроль* осуществляется в течение семестра в форме собеседования и устного опроса.

Собеседования и устные опросы направлены на проверку степени усвоения материала и понимания теоретических сведений, используемых в процессе выполнения работы. Примерные перечень вопросов для контроля знаний приведен в таблице:

Тематика дисциплины	Контрольные вопросы
Т.1. Линейные пространства над конечным полем ОПК-3.1,3.2	<ol style="list-style-type: none"> <li>1. Определение линейного пространства (ЛП) над полем. Примеры линейных пространств</li> <li>2. Определение линейной комбинации векторов ЛП. Линейно зависимые и линейно независимые системы векторов</li> <li>3. Определение базиса и размерности ЛП. Разложение вектора по базису. Число базисных векторов и количество базисов в <math>L_n</math></li> <li>4. Выражение результатов линейных операций над векторами в базисе</li> <li>5. Основные теоремы о базисе. Канонический базис</li> <li>6. Переход от одного базиса к другому. Матрица перехода</li> <li>7. Нахождение базиса системы векторов</li> <li>8. Определение линейного подпространства. Его размерность. Примеры линейных подпространств</li> <li>9. Линейная оболочка системы векторов как подпространство. Его базис и размерность</li> <li>10. Изоморфизм линейных подпространств</li> <li>11. Решение системы линейных однородных уравнений. Общее решение системы</li> <li>12. Пространства со скалярным произведением. Геометрия пространства</li> <li>13. Ортогональные и ортонормированные системы векторов. Ортогональный и ортонормированный базис. Выражение скалярного произведения: в базисе; в ортонормированном базисе</li> <li>14. Процесс ортогонализации Грамма-Шмидта</li> </ol>
Т.2. Расширенный алгоритм Евклида ОПК-3.1,3.2	<ol style="list-style-type: none"> <li>1. Ортогональное дополнение к линейному подпространству евклидова пространства</li> <li>2. Линейное пространство над конечным полем <math>X</math>. Пространство <math>Q=X^n</math>; его размерность и мощность</li> <li>3. Подпространства пространства <math>Q</math>. Порождающая и проверочная матрицы. Их канонические формы</li> <li>4. Алгоритм быстрого возведения в степень</li> <li>5. Определение и свойства функции Эйлера</li> <li>6. Приведенная система вычетов</li> <li>7. Теорема Ферма и Эйлера. Их применение</li> <li>8. Различные формы расширенного алгоритма Евклида в кольце целых чисел</li> <li>9. Расширенный алгоритм Евклида в кольце <math>Z_n</math>. Вычисление обратного элемента</li> <li>10. Расширенный алгоритм Евклида для многочленов: над полем рациональных чисел; над конечным полем <math>Z_p</math></li> </ol>
Т.3. Конечные поля (поля Галуа) ОПК-3.1,3.2	<ol style="list-style-type: none"> <li>1. Общее определение конечного поля (поля Галуа). Простые поля.</li> <li>2. Алгебраические свойства конечных полей</li> </ol>

	<ul style="list-style-type: none"> <li>3. Определение примитивного элемента конечного поля. Теорема его существования</li> <li>4. Характер конечного поля. Числа поля. Степень суммы элементов поля</li> <li>5. Основная теорема теории конечных полей. Количество элементов поля.</li> <li>6. Расширение полей с помощью неприводимого многочлена</li> <li>7. Примитивный элемент и примитивный многочлен поля <math>GF(p^m)</math></li> <li>8. Структура конечного поля</li> <li>9. Арифметика конечного поля. Операция умножения. Процедура <math>xtime</math></li> <li>10. Структура полей: <math>GF(p^2)</math>; <math>GF(p^m)</math></li> </ul>
Т.4. Применение простых чисел в криптографии ОПК-10.1	<ul style="list-style-type: none"> <li>1. Количество простых чисел. Неравенство Чебышева. Числа Ферма. Числа Мерсенны.</li> <li>2. Детерминированные и вероятностные тесты проверки чисел на простоту</li> <li>3. Критерий Вильсона. Полиномиальный тест</li> <li>4. Тест Ферма. Псевдопростые числа. Числа Кармайкла</li> <li>5. Тест «испытание квадратным корнем»</li> <li>6. Различные варианты теста Миллера-Рабина Алгоритмы генерации простых чисел с заданной разрядностью</li> <li>7. Теорема Поклингтона и ее применение для генерации простых чисел</li> <li>8. Алгоритм Маурера генерации простых чисел</li> </ul>
Т.5. Задача факторизации чисел ОПК-3.2	<ul style="list-style-type: none"> <li>1. Задача факторизации чисел. Метод пробных делений</li> <li>2. Алгоритм вычисления <math>[n]</math></li> <li>3. Метод Ферма факторизации чисел</li> <li>4. <math>\square</math> – метод Полларда факторизации чисел</li> <li>5. <math>(\square-1)</math> – метод Полларда факторизации чисел</li> </ul>
Т.6. Определение дискретного логарифма ОПК-3.2,10.1	<ul style="list-style-type: none"> <li>1. Определение дискретного логарифма в циклической мультипликативной группе. Условие его существования. Случай неединственности.</li> <li>2. <math>\rho</math> – метод Полларда вычисления дискретного логарифма</li> <li>3. Вычисление дискретного логарифма с помощью КТО (Метод Нечаева)</li> <li>4. Алгоритм «baby-step»</li> <li>5. Шифр Вернама</li> </ul>
Т.7. Определение ПСП ОПК-10.1	<ul style="list-style-type: none"> <li>1. Генераторы псевдослучайных чисел (ПСЧ)</li> <li>2. Алгоритм RC4</li> <li>3. Алгоритм RSA. Генератор ПСЧ на основе RSA</li> <li>4. Датчики M-последовательностей</li> <li>5. Тест «стопка книг»</li> </ul>

### Тестовые задания по темам.

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
1.	Линейные пространства над конечным полем ОПК-3.1,3.2	<p style="text-align: center;"><u>Задание 1.</u></p> <p>Полем <math>F</math> называется множество элементов...</p> <p><i>Выберите 1 правильный ответ</i></p> <p>1) замкнутое относительно двух операций,</p>

- называемых сложением и умножением;
- 2) не замкнутое относительно двух операций, называемых сложением и умножением;
  - 3) открытое относительно двух операций, называемых сложением и умножением;
  - 4) полуоткрытое относительно двух операций, называемых сложением и умножением.

Задание 2.

Операции сложения и умножения удовлетворяют...

*Выберите 1 правильный ответ*

- 1) 4 аксиомам;
- 2) 3 аксиомам;
- 3) 2 аксиомам;
- 4) 6 аксиомам.

Задание 3.

Теория кодирования в основном оперирует с...

*Выберите 1 правильный ответ.*

- 1) бесконечными полями;
- 2) кольцами;
- 3) группами;
- 4) конечными полями.

Задание 4.

Существуют конечные поля только порядка, равного...

*Выберите 1 правильный ответ.*

- 1) рациональной степени простого числа:  $q = p^m$ ;
- 2) целой степени простого числа:  $q = p^m$ ;
- 3) дробной степени простого числа:  $q = p^m$ ;
- 4) иррациональной степени простого числа:  $q = p^m$ .

Задание 5.

Расширенные конечные поля (порядка  $q = p^m$ , где  $m > 1$ ) не могут быть построены на основании...

*Выберите 1 правильный ответ.*

- 1) групп по  $\text{mod } q$ ;
- 2) колец по  $\text{mod } q$ ;
- 3) арифметики по  $\text{mod } q$ ;
- 4) полей по  $\text{mod } q$ .

Задание 6.

Векторным пространством  $V_F$  над полем  $F$  называется множество элементов (векторов), замкнутое относительно...

*Выберите 1 правильный ответ.*

- 1) двух операций: сложения векторов и умножения вектора на скаляр;
- 2) трех операций;
- 3) четырех операций;

		<p>4) шести операций.</p> <p style="text-align: center;"><u>Задание 7.</u></p> <p>Пусть в пространстве <math>V_F</math> имеется набор из <math>m</math> векторов <math>\mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_m</math>. Эти вектора называются линейно зависимыми, если...</p> <p><i>Выберите 1 правильный ответ.</i></p> <ol style="list-style-type: none"> <li>1) ни один не может быть представлен в виде линейной комбинации других;</li> <li>2) хотя бы один может быть представлен в виде линейной комбинации других;</li> <li>3) каждый из них должен быть представлен в виде линейной комбинации других;</li> <li>4) любые три из них могут быть представлены в виде линейной комбинации других.</li> </ol> <p style="text-align: center;"><u>Задание 8.</u></p> <p>Если ни один из векторов <math>\mathbf{g}_i</math> не является линейной комбинацией других, то вектора называются...</p> <p><i>Выберите 1 правильный ответ.</i></p> <ol style="list-style-type: none"> <li>1) линейно зависимыми;</li> <li>2) ортогональными;</li> <li>3) компланарными;</li> <li>4) линейно независимыми.</li> </ol> <p style="text-align: center;"><u>Задание 9.</u></p> <p>Максимальное число линейно независимых векторов <math>m</math> в данном пространстве называется...</p> <p><i>Выберите 1 правильный ответ.</i></p> <ol style="list-style-type: none"> <li>1) рангом;</li> <li>2) размерностью пространства;</li> <li>3) порядком;</li> <li>4) степенью.</li> </ol> <p style="text-align: center;"><u>Задание 10.</u></p> <p>Дать определение векторного подпространства.</p>
2.	Расширенный алгоритм Евклида ОПК-3.1,3.2	<p style="text-align: center;"><u>Задание 1.</u></p> <p>Расширенный алгоритм Евклида — это расширение алгоритма Евклида, которое...</p> <p><i>Выберите 1 правильный ответ.</i></p> <ol style="list-style-type: none"> <li>1) вычисляет только наибольший общий делитель (НОД) целых чисел <math>a</math> и <math>b</math>;</li> <li>2) вычисляет кроме наибольшего общего делителя (НОД) целых чисел <math>a</math> и <math>b</math> ещё и наименьшее кратное этих же чисел;</li> <li>3) вычисляет три общих делителя целых чисел <math>a</math> и <math>b</math>;</li> <li>4) вычисляет кроме наибольшего общего делителя (НОД) целых чисел <math>a</math> и <math>b</math> ещё и коэффициенты соотношения Безу.</li> </ol> <p style="text-align: center;"><u>Задание 2.</u></p>

Расширенный алгоритм Евклида особенно полезен, когда  $a$  и  $b$ ...

*Выберите 1 правильный ответ.*

- 1) составные числа;
- 2) взаимно простые;
- 3) есть делителями одно и другого;
- 4) есть кратными некоторого числа.

Задание 3.

Пара коэффициентов Безу, которую даёт расширенный алгоритм Евклида, является...

*Выберите 1 правильный ответ.*

- 1) максимальной парой коэффициентов Безу;
- 2) свободной парой коэффициентов Безу;
- 3) собственной парой коэффициентов Безу;
- 4) минимальной парой коэффициентов Безу.

Задание 4.

Если  $a$  и  $b$  – два ненулевых многочлена, то расширенный алгоритм Евклида даёт...

*Выберите 1 правильный ответ.*

- 1) единственную пару многочленов  $(s,t)$ ;
- 2) нулевую пару многочленов  $(s,t)$ ;
- 3) две пары многочленов  $(s,t)$ ;
- 4) наибольшую пару многочленов  $(s,t)$ .

Задание 5.

Деление  $\frac{a}{b}$  находится в канонической упрощённой форме, если...

*Выберите 1 правильный ответ.*

- 1)  $a$  и  $b$  взаимно простые и  $b$  отрицательно;
- 2)  $a$  и  $b$  взаимно простые и  $b$  равно нулю;
- 3)  $a$  и  $b$  взаимно простые и  $b$  положительно;
- 4)  $a$  и  $b$  не простые числа и  $b$  положительно.

Задание 6.

Соотношение Безу утверждает, что  $a$  и  $n$  взаимно простые тогда и только тогда, когда...

*Выберите 1 правильный ответ.*

- 1) существуют целые  $s$  и  $t$ , такие что
- 2) существуют целые  $s$  и  $t$ , такие что
- 3) существуют целые  $s$  и  $t$ , такие что
- 4) существуют целые  $s$  и  $t$ , такие что

Задание 7.

Линейный код  $U$  имеет минимальное расстояние, равное  $d$ , тогда и только тогда, когда...

*Выберите 1 правильный ответ.*

- 1) проверочная матрица  $H$  содержит множество из  $d$  линейно независимых столбцов, а любое множество из  $d - 1$  столбцов матрицы  $H$  линейно

зависимо;

- 2) проверочная матрица **H** содержит множество из  $d$  линейно зависимых столбцов, а любое множество из  $d - 1$  столбцов матрицы **H** линейно независимо;
- 3) проверочная матрица **H** содержит множество из  $d$  линейно зависимых столбцов, а любое множество из  $d - 1$  столбцов матрицы **H** линейно зависимо;
- 4) проверочная матрица **H** содержит множество из  $d$  линейно независимых столбцов, а любое множество из  $d - 1$  столбцов матрицы **H** линейно независимо.

Задание 8.

Два кода эквивалентны тогда и только тогда, когда их порождающие матрицы...

*Выберите 1 правильный ответ.*

- 1) получаются одна из другой посредством перестановки столбцов либо в результате неэлементарных операций над строками;
- 2) получаются одна из другой посредством перестановки строк либо в результате элементарных операций над строками;
- 3) получаются одна из другой посредством перестановки столбцов либо в результате применения тензорных операций над матрицами;
- 4) получаются одна из другой посредством перестановки столбцов либо в результате элементарных операций над строками.

Задание 9.

Минимальное расстояние (минимальный вес) любого линейного  $(n, k)$  кода удовлетворяет...

*Выберите 1 правильный ответ.*

- 1) неравенству:  $d \leq n - k + 1$ ;
- 2) равенству нулю;
- 3) равенству 1;
- 4) равенству 2.

Задание 10.

Сформулировать теорему о границе Синглтона.



3.	<p>Конечные поля (поля Галуа) ОПК-3.1,3.2</p>	<p style="text-align: center;"><u>Задание 1.</u></p> <p>Конечным полем или полем Галуа в общей алгебре называется поле...</p> <p><i>Выберите 1 правильный ответ.</i></p> <ol style="list-style-type: none"> <li>1) состоящее из бесконечного числа элементов, которое называется порядком поля;</li> <li>2) состоящее из конечного числа элементов, которое называется рангом поля;</li> <li>3) состоящее из конечного числа элементов, которое называется порядком поля;</li> <li>4) состоящее из бесконечного числа элементов, которое называется степенью поля.</li> </ol> <p style="text-align: center;"><u>Задание 2.</u></p> <p>Конечное поле обычно обозначается...</p> <p><i>Выберите 1 правильный ответ.</i></p> <ol style="list-style-type: none"> <li>1) <math>GF(q)</math>; 2) <math>GF(q) &gt; 2</math>; 3) <math>GF(q) &gt; 4</math>; 4) <math>GF(q) \neq 0</math></li> </ol> <p style="text-align: center;"><u>Задание 3.</u></p> <p>Конечным полем называется конечное множество, на котором определены произвольные операции...</p> <p><i>Выберите 1 правильный ответ.</i></p> <ol style="list-style-type: none"> <li>1) сложение и деление (кроме деления на 0) в соответствии с аксиомами поля;</li> <li>2) сложение, умножение, вычитание и деление (кроме деления на 0) в соответствии с аксиомами поля;</li> <li>3) умножение, вычитание и деление (кроме деления на 0) в соответствии с аксиомами поля;</li> <li>4) сложение, умножение (кроме деления на 0) в соответствии с аксиомами поля.</li> </ol> <p style="text-align: center;"><u>Задание 4.</u></p> <p>Любое поле простого порядка может быть представлено...</p> <p><i>Выберите 1 правильный ответ.</i></p> <ol style="list-style-type: none"> <li>1) полем вычетов; 2) группой вычетов;</li> <li>3) подгруппой вычетов; 4) кольцом вычетов.</li> </ol> <p style="text-align: center;"><u>Задание 5.</u></p> <p>Только когда порядком есть простое число, кольцо вычетов...</p> <p><i>Выберите 1 правильный ответ.</i></p> <ol style="list-style-type: none"> <li>1) есть кольцом;</li> <li>2) есть полем;</li> <li>3) есть группой;</li> <li>4) есть подгруппой.</li> </ol> <p style="text-align: center;"><u>Задание 6.</u></p> <p>Характеристика каждого конечного поля является...</p> <p><i>Выберите 1 правильный ответ.</i></p>
----	---	---

		<p>1) дробным числом; 2) рациональным числом; 3) простым числом; 4) иррациональным числом. <u>Задание 7.</u> Для каждого простого числа и натурального числа существует... <i>Выберите 1 правильный ответ.</i> 1) конечное кольцо из <math>p^n</math> элементов; 2) конечное поле из <math>p^n</math> элементов; 3) конечная группа из <math>p^n</math> элементов; 4) конечная подгруппа из <math>p^n</math> элементов; <u>Задание 8.</u> Кольцом <math>\langle R, +, * \rangle</math> называется множество <math>R</math> с двумя бинарными операциями <math>+</math> и <math>*</math> <i>Выберите 1 правильный ответ.</i> 1) с двумя бинарными операциями <math>+</math> и <math>-</math> 2) с двумя бинарными операциями <math>-</math> и <math>*</math> 3) с одной бинарной операцией <math>+</math>; 4) с двумя бинарными операциями <math>+</math> и <math>*</math>; <u>Задание 9.</u> В математике криптографии есть теорема ... <i>Выберите 1 правильный ответ.</i> 1) Фалеса; 2) Веддерберна; 3) Лагранжа; 4) Даламбера. <u>Задание 10.</u> Если <math>p</math> — простое, то <math>Z_p</math> ... <i>Выберите 1 правильный ответ.</i> 1) конечное поле; 2) конечное кольцо; 3) конечная группа; 4) конечная подгруппа.</p>
4.	Применение простых чисел в криптографии ОПК-10.1	<p><u>Задание 1.</u> Теорема о существовании неприводимых многочленов. Для каждого конечного поля <math>F</math> и каждого натурального <math>n</math> в кольце <math>F[x]</math> существует... <i>Выберите 1 правильный ответ.</i> 1) неприводимое поле степени <math>n</math>; 2) неприводимое кольцо степени <math>n</math>; 3) неприводимый многочлен степени <math>n</math>; 4) неприводимое кольцо порядка <math>n</math>. <u>Задание 2.</u> Подмножество <math>K \subseteq F</math> называется подполем поля <math>\langle F, +, * \rangle</math>, если <math>\langle K, +, * \rangle</math> ... <i>Выберите 1 правильный ответ.</i></p>

- 1) само является полем;
- 2) является кольцом;
- 3) является группой;
- 4) является подгруппой.

Задание 3.

Поле, которое не содержит собственных подполей, называется...

*Выберите 1 правильный ответ.*

- 1) составным;
- 2) квадратичным;
- 3) кубическим;
- 4) простым.

Задание 4.

Размерность векторного пространства  $F$  над  $K$  называется...

*Выберите 1 правильный ответ.*

- 1) степенью многочлена;
- 2) степенью расширения;
- 3) порядком многочлена;
- 4) порядком расширения.

Задание 5.

Многие важнейшие помехоустойчивые коды систем связи, в частности циклические, основаны на структурах...

*Выберите 1 правильный ответ.*

- 1) конечных полей Лагранжа;
- 2) конечных полей Галуа;
- 3) конечных колец Галуа;
- 4) конечных групп Галуа.

Задание 6.

Циклическим кодом называется линейный блочный  $(n,k)$ -код, который характеризуется свойством...

*Выберите 1 правильный ответ.*

- 1) коммутативности;
- 2) ассоциативности;
- 3) цикличности;
- 4) дистрибутивности.

Задание 7.

В циклическом коде кодовые слова представляют...

*Выберите 1 правильный ответ.*

- 1) группами;
- 2) полями;
- 3) кольцами;
- 4) многочленами (полиномами).

Задание 8.

Коды Рида — Соломона базируются на...

		<p><i>Выберите 1 правильный ответ.</i></p> <ol style="list-style-type: none"> <li>1) полях Галуа;</li> <li>2) кольцах;</li> <li>3) группах Абеля;</li> <li>4) многочленах.</li> </ol> <p style="text-align: center;"><u>Задание 9.</u></p> <p>Турбокодом называют параллельную структуру сигнала, состоящую...</p> <p><i>Выберите 1 правильный ответ.</i></p> <ol style="list-style-type: none"> <li>1) из систематического кодов;</li> <li>2) из двух или большего числа систематических кодов;</li> <li>3) из двух или большего числа псевдокодов;</li> <li>4) только из двух систематических кодов.</li> </ol> <p style="text-align: center;"><u>Задание 10.</u></p> <p>Дайте понятие простого числа.</p>
5.	Задача факторизации чисел ОПК-3.2	<p style="text-align: center;"><u>Задание 1.</u></p> <p>Любое составное число может быть представлено в виде...</p> <p><i>Выберите 1 правильный ответ.</i></p> <ol style="list-style-type: none"> <li>1) единственно возможного произведения составных чисел;</li> <li>2) единственно возможного произведения простых чисел;</li> <li>3) нескольких вариантов произведения простых чисел;</li> <li>4) нескольких вариантов произведения составных чисел.</li> </ol> <p style="text-align: center;"><u>Задание 2.</u></p> <p>Любое составное число может быть представлено в виде единственно возможного произведения простых чисел. Это теорема...</p> <p><i>Выберите 1 правильный ответ.</i></p> <ol style="list-style-type: none"> <li>1) Абеля;</li> <li>2) Архимеда;</li> <li>3) Аристотеля;</li> <li>4) Евклида.</li> </ol> <p style="text-align: center;"><u>Задание 3.</u></p> <p>Идея асимметричного шифрования, или «шифрования с открытым ключом» принадлежит....</p> <p><i>Выберите 1 правильный ответ.</i></p> <ol style="list-style-type: none"> <li>1) Уитфилду Диффи и Мартину Хеллману;</li> <li>2) Эдиссону;</li> <li>3) Абелю;</li> <li>4) Евклиду.</li> </ol> <p style="text-align: center;"><u>Задание 4.</u></p>

		<p>Алгоритм шифрования RSA разработан....  <i>Выберите 1 правильный ответ.</i></p> <ol style="list-style-type: none"> <li>1) Уитфилду Диффи и Мартину Хеллману;</li> <li>2) Роном Ривестом, Ади Шамиром и Леном Адлеманом;</li> <li>3) Евклидом;</li> <li>4) Абелем.</li> </ol> <p style="text-align: center;"><u>Задание 5.</u></p> <p>Для применения алгоритма RSA требуется построить...  <i>Выберите 1 правильный ответ.</i></p> <ol style="list-style-type: none"> <li>1) 2 открытых ключа;</li> <li>2) открытый и секретный ключи;</li> <li>3) 2 секретных ключа;</li> <li>4) 2 открытых и 1 секретный ключи.</li> </ol> <p style="text-align: center;"><u>Задание 6.</u></p> <p>Опишите задачу факторизации чисел. Метод пробных делений.</p> <p style="text-align: center;"><u>Задание 7.</u></p> <p>Опишите алгоритм вычисления <math>[\rho_n]</math>.</p> <p style="text-align: center;"><u>Задание 8.</u></p> <p>Опишите метод Ферма факторизации чисел.</p> <p style="text-align: center;"><u>Задание 9.</u></p> <p>Опишите <math>\rho</math> – метод Полларда факторизации чисел.</p> <p style="text-align: center;"><u>Задание 10.</u></p> <p>Опишите <math>(\rho - 1)</math> – метод Полларда факторизации чисел.</p>
6.	<p>Определение дискретного логарифма  ОПК-3.2,10.1</p>	<p style="text-align: center;"><u>Задание 1.</u></p> <p>Дайте определение дискретного логарифма в циклической мультипликативной группе.</p> <p style="text-align: center;"><u>Задание 2.</u></p> <p>Условие существования дискретного логарифма в циклической мультипликативной группе. Случай неединственности.</p> <p style="text-align: center;"><u>Задание 3.</u></p> <p>Опишите <math>\rho</math> – метод Полларда вычисления дискретного логарифма.</p> <p style="text-align: center;"><u>Задание 4.</u></p> <p>Опишите метод вычисления дискретного логарифма с помощью КТО (Метод Нечаева).</p> <p style="text-align: center;"><u>Задание 5.</u></p> <p>Опишите алгоритм «baby-step».</p> <p style="text-align: center;"><u>Задание 6.</u></p> <p>Опишите шифр Вернама</p>

7.	Определение ПСП ОПК-10.1	<p style="text-align: center;"><u>Задание 1.</u></p> <p>Опишите генераторы псевдослучайных чисел (ПСЧ).</p> <p style="text-align: center;"><u>Задание 2.</u></p> <p>Опишите алгоритм RC4.</p> <p style="text-align: center;"><u>Задание 3.</u></p> <p>Опишите алгоритм RSA.</p> <p style="text-align: center;"><u>Задание 4.</u></p> <p>Опишите генератор ПСЧ на основе RSA.</p> <p style="text-align: center;"><u>Задание 5.</u></p> <p>Опишите датчики M-последовательностей.</p> <p style="text-align: center;"><u>Задание 6.</u></p> <p>Опишите тест «стопка книг».</p>
----	-----------------------------	---

#### 5.4. Описание критериев оценивания компетенций и шкалы оценивания

При промежуточной аттестации в форме экзамена используется следующая шкала оценивания: 2 – неудовлетворительно, 3 – удовлетворительно, 4 – хорошо, 5 – отлично.

Критериями оценивания достижений показателей являются:

Наименование показателя оценивания результата обучения по дисциплине	Критерий оценивания
Знания	Знание терминов, определений, понятий
	Знание основных закономерностей, соотношений, принципов
	Объем освоенного материала
	Полнота ответов на вопросы
	Четкость изложения и интерпретации знаний
Умения	Умение анализировать основные положения законодательства в области безопасности информации
	Умение использовать руководящие документы регуляторов в области информационной безопасности
Навыки	Владение навыками теоретического и экспериментального исследования объектов профессиональной деятельности
	Качество выполнения исследований объектов профессиональной деятельности
	Самостоятельность выполнения исследований объектов профессиональной деятельности

Оценка преподавателем выставляется интегрально с учётом всех показателей и критериев оценивания.

Оценка сформированности компетенций по показателю Знания.

Критерий	Уровень освоения и оценка			
	2	3	4	5
Знание терминов, определений,	Не знает терминов и	Знает термины и определения, но	Знает термины и определения	Знает термины и определения, может

понятий	определений	допускает неточности формулировок		корректно сформулировать их самостоятельно
Знание основных закономерностей, соотношений, принципов	Не знает основные закономерности и соотношения, принципы построения знаний	Знает основные закономерности, соотношения, принципы построения знаний	Знает основные закономерности, соотношения, принципы построения знаний, их интерпретирует и использует	Знает основные закономерности, соотношения, принципы построения знаний, может самостоятельно их получить и использовать
Объем освоенного материала	Не знает значительной части материала дисциплины	Знает только основной материал дисциплины, не усвоил его деталей	Знает материал дисциплины в достаточном объеме	Обладает твердым и полным знанием материала дисциплины, владеет дополнительными знаниями
Полнота ответов на вопросы	Не дает ответы на большинство вопросов	Дает неполные ответы на все вопросы	Дает ответы на вопросы, но не все - полные	Дает полные, развернутые ответы на поставленные вопросы
Четкость изложения и интерпретации знаний	Излагает знания без логической последовательности	Излагает знания с нарушениями в логической последовательности	Излагает знания без нарушений в логической последовательности	Излагает знания в логической последовательности, самостоятельно их интерпретируя и анализируя
	Не иллюстрирует изложение поясняющими схемами, рисунками и примерами	Выполняет поясняющие схемы и рисунки небрежно и с ошибками	Выполняет рисунки и схемы корректно и понятно	Выполняет поясняющие рисунки и схемы точно и аккуратно, раскрывая полноту усвоенных знаний
	Неверно излагает и интерпретирует знания	Допускает неточности в изложении и интерпретации знаний	Грамотно и по существу излагает знания	Грамотно и точно излагает знания, делает самостоятельные выводы

### Оценка сформированности компетенций по показателю Умения.

Критерий	Уровень освоения и оценка			
	2	3	4	5
Умение анализировать основные математические методы криптографических преобразований информации	Не умеет анализировать основные математические методы криптографических преобразований информации	Допускает неточности в анализе основных математических методов криптографических преобразований информации	Умеет анализировать основные математические методы криптографических преобразований информации	Умеет анализировать основные математические методы криптографических преобразований информации и делать обобщающие выводы
Умение осуществлять обоснованный выбор	Не умеет осуществлять обоснованный выбор	Осуществление обоснованного выбора	Осуществляет обоснованный выбор математическ	Умело осуществляет обоснованный выбор

выбор математических методов для решения типовых задач	математических методов для решения типовых задач	математических методов для решения типовых задач вызывает затруднения	их методов для решения типовых задач	математических методов для решения типовых задач
--	--	---	--------------------------------------	--

Оценка сформированности компетенций по показателю Навыки.

Критерий	Уровень освоения и оценка			
	2	3	4	5
Владение навыками теоретического и экспериментального исследования объектов профессиональной деятельности	Не владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности	Не достаточно хорошо владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности	Владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности	Профессионально владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности
Качество выполнения исследований объектов профессиональной деятельности	Не качественно выполняет исследования объектов профессиональной деятельности, допускает грубые ошибки	Не достаточно качественно выполняет исследования объектов профессиональной деятельности, допускает и исправляет ошибки с посторонней помощью	Не достаточно качественно выполняет исследования объектов профессиональной деятельности, допускает и исправляет ошибки самостоятельно	Качественно выполняет исследования объектов профессиональной деятельности
Самостоятельность выполнения исследований объектов профессиональной деятельности	Не может самостоятельно выполнять исследования объектов профессиональной деятельности	Выполняет исследования объектов профессиональной деятельности с посторонней помощью	При выполнении исследования объектов профессиональной деятельности иногда требуется посторонняя помощь	Самостоятельно выполняет исследования объектов профессиональной деятельности



## **6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ**

### **6.1. Материально-техническое обеспечение**

№	Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы
1.	Учебная аудитория для проведения лекционных занятий	Специализированная мебель. Мультимедийная установка, экран, доски
2.	Учебная аудитория для проведения практических занятий	Специализированная мебель. Компьютеры на базе процессоров Intel или AMD.
3.	Читальный зал библиотеки для самостоятельной работы	Специализированная мебель. Компьютерная техника, подключенная к сети интернет и имеющая доступ в электронно-образовательную среду.

### **6.2. Лицензионное и свободно распространяемое программное обеспечение**

№	Перечень лицензионного программного обеспечения.	Реквизиты подтверждающего документа
1	Microsoft Windows 10 Корпоративная	(Соглашение Microsoft Open Value Subscription V9221014 Соглашение действительно с 01.11.2020 по 31.10.2023). Договор поставки ПО № 128-21 от 30.10.2021.
2	Microsoft Office Professional Plus 2016	(Соглашение Microsoft Open Value Subscription V9221014 Соглашение действительно с 01.11.2020 по 31.10.2023). Договор поставки ПО № 128-21 от 30.10.2021.
3	Kaspersky Endpoint Security «Стандартный Russian Edition»	Сублицензионный договор № 102 от 24.05.2018. Срок действия лицензии до 19.08.2020 Гражданско-правовой Договор (Контракт) № 27782 «Поставка продления права пользования (лицензии) Kaspersky Endpoint Security от 03.06.2020. Срок действия лицензии 19.08.2022г.
4	Среды программирования Free Pascal, Dev C++ или CodeBlocks	Свободно распространяемое ПО согласно условиям лицензионного соглашения

### 6.3. Перечень учебных изданий и учебно-методических материалов

1. Сергиенко Е.Н. Математика криптографии: методические указания к выполнению лабораторных работ для студентов специальности 090303.65 – Информационная безопасность / сост. Е.Н. Сергиенко, С.А. Панарин, И.А. Пригорнев, А.С. Чурилов. – Белгород: Изд-во БГТУ, 2014. – 59 с.
2. Василенко О. Н. Теоретико- числовые алгоритмы в криптографии – 2 издание., доп. / О. Н. Василенко. – М.: МЦНМО, 2006. – 363 с.
3. Зензин О. С. Стандарт криптографической защиты – AES. Конечные поля. /О.С. Зензин М. А Иванов. – М.: Кудиц – Образ, 2002. – 174 с.
4. Математические и компьютерные основы криптографии: учебное пособие. / Ю. С. Харин, В. И Берник, Г. В. Матвеев, С. В. Авчиев. – Минск.: Новое знание, 2003. – 381 с.
5. Маховенко Е. Б. Теоретико-числовые методы криптографии. / Е. Б. Маховенко. – М.: Гелиос АРВ, 2006. – 320 с.
6. Смарт Н. Криптография / Н. Смарт. – М.: Техносфера, 2005. – 255 с.
7. Фороузан Б. А. Криптография и безопасность сетей. / Б. А. Фороузан Курош. – М.: Бином, 2010. – 784 с.
8. Алешников С.И. Математические методы защиты информации. Часть 3. Вычислительный практикум по числовым полям и криптографии в квадратичных полях: Практическое пособие – Калининград: Российский государственный университет им. Иммануила Канта, 2006. Эл. ресурс: <http://www.iprbookshop.ru/23851.html>
9. Романьков В.А. Алгебраическая криптография: Монография – Омск: Омский государственный университет, 2013. Эл. ресурс: <http://www.iprbookshop.ru/24868.html>
10. Бабаш А. В. Криптография: учебное пособие. / А. В. Бабаш, Г. П. Шанкин. – М.: Солон – Р, 2002. – 511 с.
11. Баричев, С. Г. Основы современной криптографии: учебный курс. / С. Г. Баричев, В. В. Гончаров, Р. Е Серов – 2 издание., перераб. и доп. – М.: Горячая линия – Телеком, 2002. – 175 с.
12. Глухов М. М., Круглов И. А., Пичкур А. Б., Черемушкин А. В. Введение в теоретико-числовые методы криптографии / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. – СПб.: Краснодар Лань, 2011. – 400 с.
13. Колесник В. Д., Кодирование при передаче и хранении информации (алгебраическая теория блоковых кодов) / В. Д. Колесник. – М.: Высшая школа, 2009. – 550 с.
14. Молдовян Н. А Практикум по криптосистемам с открытым ключом. / Н. А. Молдовян. – СПб.: БХВ – Петербург, 2007. – 304 с.
15. Применко Э. А. Алгебраические основы криптографии. / Э. А. Применко. – М.: Мир, 2006. – 471 с.
16. Рябко Б. Я., Фионов А. Н., Криптографические методы защиты информации. / Б. Я. Рябко, А. Н. Фионов. – М.: Горячая линия – Телеком, 2005. – 229 с.
17. Столлингс В. Криптография и защита сетей: принципы и практика / В. Столлингс – 2 издание. – М.: Вильямс – Р, 2001. – 381 с.
18. Тилборг ван Х. К. А. Основы криптологии. / Х. К. А. ван Тилберг. – М.:

Мир, 2006. – 471 с.

19. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ / Б. Шнайер. – М.: Триумф, 2003. – 815 с.

#### **6.4. Перечень интернет ресурсов, профессиональных баз данных, информационно-справочных систем**

1. Электронная библиотека (на базе ЭБС «БиблиоТех») — Режим доступа: <http://ntb.bstu.ru>
2. Электронно-библиотечная система IPRbooks — Режим доступа: <http://www.iprbookshop.ru>
3. Электронно-библиотечная система «Университетская библиотека ONLINE» — Режим доступа: <http://www.biblioclub.ru/>

## 7. УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ

Рабочая программа утверждена на 202\_\_/202\_\_ учебный год  
без изменений / с изменениями, дополнениями

Протокол № \_\_\_\_\_ заседания кафедры от « \_\_\_\_ » \_\_\_\_\_ 202\_\_ г.

Заведующий кафедрой \_\_\_\_\_  
подпись, ФИО

Директор института \_\_\_\_\_  
подпись, ФИО