

**МИНОБРНАУКИ РОССИИ**  
федеральное государственное бюджетное образовательное учреждение высшего образования  
**«Кузбасский государственный технический университет имени Т.Ф. Горбачева»**

Филиал КузГТУ в г. Новокузнецке

**УТВЕРЖДАЮ**  
Директор филиала КузГТУ  
\_\_\_\_\_ Т.А. Евсина  
«29» мая 2023 г.

**Рабочая программа дисциплины**  
**Криптографические средства защиты информации**

Специальность  
«10.02.05 Обеспечение информационной безопасности автоматизированных систем»

Присваиваемая квалификация  
«Техник по защите информации»

Форма обучения  
очная

Год набора 2023

Срок обучения на базе  
среднего общего образования – 2 года 10 месяцев

Новокузнецк 2023 г.

**РАБОЧУЮ ПРОГРАММУ СОСТАВИЛ**

Преподаватель отделения СПО

  
Подпись

С.А. Строкин

**СОГЛАСОВАНО**

заведующий отделением СПО

  
Подпись

Е.В. Севостьянова

**СОГЛАСОВАНО**

Зам. директора по УР

  
Подпись

Т.А. Евсина

Рабочая программа обсуждена на заседании  
учебно-методического совета филиала КузГТУ в г. Новокузнецке  
Протокол №6 от 29мая 2023 года

## 1. Общая характеристика рабочей программы дисциплины

### 1.1 Место дисциплины в структуре основной образовательной программы

Учебная дисциплина «Криптографические средства защиты информации» является обязательной частью профессионального цикла основной образовательной программы в соответствии с ФГОС по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

Учебная дисциплина «Криптографические средства защиты информации» обеспечивает формирование профессиональных и общих компетенций в соответствии с ФГОС по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

### 1.2 Цель и планируемые результаты освоения дисциплины, соотнесенные с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:  
общих компетенций:

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

Знать: способы решения задач профессиональной деятельности, применительно к различным контекстам;

Уметь: выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам;

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

Знать: источники, включая электронные ресурсы, медиаресурсы, Интернетресурсы, периодические издания по специальности для решения профессиональных задач;

Уметь: использовать различные источники, включая электронные ресурсы, медиаресурсы, Интернетресурсы, периодические издания по специальности для решения профессиональных задач;

ОК 09. Использовать информационные технологии в профессиональной деятельности.

Знать: информационно-коммуникационные технологии профессиональной деятельности;

Уметь: использовать информационные технологии в профессиональной деятельности;

профессиональных компетенций:

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.

Знать: основные понятия криптографии и типовых криптографических методов и средств защиты информации;

Уметь: применять математический аппарат для выполнения криптографических преобразований; использовать типовые программные криптографические средства, в том числе электронную подпись; Иметь практический опыт: применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных; учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности;

### В результате освоения дисциплины обучающийся в общем по дисциплине должен

Знать:

- способы решения задач профессиональной деятельности, применительно к различным контекстам;
- источники, включая электронные ресурсы, медиаресурсы, Интернетресурсы, периодические издания по специальности для решения профессиональных задач;
- информационно-коммуникационные технологии профессиональной деятельности;
- основные понятия криптографии и типовых криптографических методов и средств защиты информации;

Уметь:

- выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам;
- использовать различные источники, включая электронные ресурсы, медиаресурсы, Интернетресурсы, периодические издания по специальности для решения профессиональных задач;
- использовать информационные технологии в профессиональной деятельности;
- применять математический аппарат для выполнения криптографических преобразований; использовать типовые программные криптографические средства, в том числе электронную подпись;

Иметь практический опыт:

- применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных; учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности;

## 2. Структура и содержание дисциплины

### 2.1 Объем дисциплины и виды учебной работы

Форма обучения	Количество часов		
	ОФ	ЗФ	ОЗФ
Курс 2 / Семестр 3			
Объем дисциплины	120		
в том числе:			
лекции, уроки	50		

Форма обучения	Количество часов		
	ОФ	ЗФ	ОЗФ
лабораторные работы			
практические занятия	40		
Консультации	6		
Самостоятельная работа	18		
Промежуточная аттестация	6		
Индивидуальное проектирование			
<b>Форма промежуточной аттестации</b>	экзамен		

## 2.2 Тематический план и содержание дисциплины

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
<b>Введение.</b>		
<i>Лекции</i>		
	Предмет и задачи криптографии. История криптографии. Основные термины.	1
	<i>Самостоятельная работа обучающихся:</i> История развития криптографии	1
<b>Раздел 1. Математические основы защиты информации</b>		
<b>Тема 1.1. Математические основы криптографии</b>		
<i>Лекции</i>		
	Лекция 1.1.1. Элементы теории множеств. Группы, кольца, поля.	1
	Лекция 1.1.2. Делимость чисел. Признаки делимости. Простые и составные числа.	1
	Лекция 1.1.3. Основная теорема арифметики. Наибольший общий делитель. Взаимно простые числа. Алгоритм Евклида для нахождения НОД.	1
	Лекция 1.1.4. Отношения сравнимости. Свойства сравнений. Модулярная арифметика.	1
	Лекция 1.1.5. Классы. Полная и приведенная система вычетов. Функция Эйлера. Теорема Ферма-Эйлера. Алгоритм быстрого возведения в степень по модулю.	1
	Лекция 1.1.6. Сравнения первой степени. Линейные диофантовы уравнения. Расширенный алгоритм Евклида.	1
	Лекция 1.1.7. Китайская теорема об остатках.	1
	Лекция 1.1.8. Проверка чисел на простоту. Алгоритмы генерации простых чисел. Метод пробных делений. Решето Эратосфена.	1
	Лекция 1.1.9. Разложение числа на множители. Алгоритмы факторизации. Факторизация Ферма. Метод Полларда.	1
	Лекция 1.1.10. Алгоритмы дискретного логарифмирования. Метод Полларда. Метод Шорра.	1
	Лекция 1.1.11. Арифметические операции над большими числами.	1
	Лекция 1.1.12. Эллиптические кривые и их приложения в криптографии.	1

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
<i>Практические занятия</i>		
	Практическое занятие 1.1.1. Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений	1
	Практическое занятие 1.1.2. Проверка чисел на простоту	1
	Практическое занятие 1.1.3. Решение задач с элементами теории чисел.	1
<i>Самостоятельная работа обучающихся</i>		
	1.1.1. Программная реализация классических шифров	2
<b>Раздел 2. Классическая криптография</b>		
<b>Тема 2.1. Методы криптографической защиты информации</b>		
<i>Лекции</i>		
	Лекция 2.1. Классификация основных методов криптографической защиты. Методы симметричного шифрования	1
	Лекция 2.1. Шифры замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр	1
	Лекция 2.3. Методы перестановки. Табличная перестановка, маршрутная перестановка. Гаммирование. Гаммирование с конечной и бесконечной гаммами	1
<i>Практические занятия</i>		
	Практическое занятие 2.1.1. Применение классических шифров замены	1
	Практическое занятие 2.1.2. Применение классических шифров перестановки	1
	Практическое занятие 2.1.3. Применение метода гаммирования	1
<i>Самостоятельная работа обучающихся</i>		
	2.1.1. Программная реализация классических шифров	2
<b>Тема 2.2. Криптоанализ</b>		
<i>Лекции</i>		
	Лекция 2.2.1. Основные методы криптоанализа. Криптографические атаки.	1
	Лекция 2.2.2. Криптографическая стойкость. Абсолютно стойкие криптосистемы. Принципы Киркхоффа	1
	Лекция 2.2.3. Перспективные направления криптоанализа, квантовый криптоанализ.	1
<i>Практические занятия</i>		
	Практическое занятие 2.2.1. Криптоанализ шифра простой замены методом анализа частотности символов	1
	Практическое занятие 2.2.2. Криптоанализ классических шифров методом полного перебора ключей	1

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
	Практическое занятие 2.2.3. Криптоанализ шифра Вижинера	2
<i>Самостоятельная работа обучающихся</i>		
	2.2.1. Оптимизация методов частотного анализа моноалфавитных шифров.1	2
<b>Тема 2.3. Поточные шифры и генераторы псевдослучайных чисел</b>		
<i>Лекции</i>		
	Лекция 2.3.1. Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии	1
	Лекция 2.3.2. Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод VBS.	1
<i>Практические занятия</i>		
	Практическое занятие 2.3.1. Применение методов генерации ПСЧ	2
<b>Раздел 3. Современная криптография</b>		
<b>Тема 3.1. Кодирование информации. Компьютеризация шифрования.</b>		
<i>Лекции</i>		
	Лекция 3.1.1. Кодирование информации. Символьное кодирование. Смысловое кодирование. Механизация шифрования. Представление информации в двоичном коде. Таблица ASCII	1
	Лекция 3.1.2. Компьютеризация шифрования. Аппаратное и программное шифрование Стандартизация программно-аппаратных криптографических систем и средств. Изучение современных программных и аппаратных криптографических средств	1
<i>Практические занятия</i>		
	Практическое занятие 3.1.1. Кодирование информации	2
	Практическое занятие 3.1.2. Программная реализация классических шифров	2
	Практическое занятие 3.1.3.Изучение реализации классических шифров замены и перестановки в программе СгурTool или аналоге.	2
<i>Самостоятельная работа обучающихся</i>		
	3.1.1. Методы механизации шифрования	2
<b>Тема 3.2. Симметричные системы шифрования</b>		
<i>Лекции</i>		
	Лекция 3.2.1. Общие сведения. Структурная схема симметричных криптографических систем	1
	Лекция 3.2.2. Отечественные алгоритмы Магма и Кузнечик и стандарты ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015. Симметричные алгоритмы DES, AES, ГОСТ 28147-89, RC4	1

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
<i>Практические занятия</i>		
	Практическое занятие 3.2.1. Изучение программной реализации современных симметричных шифров	2
<i>Самостоятельная работа обучающихся</i>		
	3.2.1. Анализ современных симметричных криптоалгоритмов	1
	3.2.2. Цифровое представление различных форм информации	1
<b>Тема 3.3. Асимметричные системы шифрования</b>		
<i>Лекции</i>		
	Лекция 3.3.1. Криптосистемы с открытым ключом. Необратимость систем. Структурная схема шифрования с открытым ключом.	1
	Лекция 3.3.2. Элементы теории чисел в криптографии с открытым ключом.	1
<i>Практические занятия</i>		
	Практическое занятие 3.3.1. Применение различных асимметричных алгоритмов.	2
	Практическое занятие 3.3.2. Изучение программной реализации асимметричного алгоритма RSA	2
<i>Самостоятельная работа обучающихся</i>		
	3.3.1. Анализ современных асимметричных криптоалгоритмов	1
<b>Тема 3.4. Аутентификация данных. Электронная подпись</b>		
<i>Лекции</i>		
	Лекция 3.4.1. Аутентификация данных. Общие понятия. ЭП. MAC. Однонаправленные хеш-функции. Алгоритмы цифровой подписи	1
<i>Практические занятия</i>		
	Практическое занятие 3.4.1. Применение различных функций хеширования, анализ особенностей хешей	2
	Практическое занятие 3.4.2. Применение криптографических атак на хеш-функции.	2
	Практическое занятие 3.4.3. Изучение программно-аппаратных средств, реализующих основные функции ЭП	2
<i>Самостоятельная работа обучающихся</i>		
	3.4.1. Сравнительный анализ функций хеширования	1
	3.4.2. Аутентификация сообщений	1
<b>Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации</b>		
<i>Лекции</i>		
	Лекция 3.5.1 Алгоритмы распределения ключей с применением симметричных и	1

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
	асимметричных схем Протоколы аутентификации. Взаимная аутентификация. Односторонняя аутентификация	
<i>Практические занятия</i>		
	Практическое занятие 3.5.1. Применение протокола Диффи-Хеллмана для обмена ключами шифрования.	2
	Практическое занятие 3.5.2. Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos.	2
<b>Тема 3.6. Криптозащита информации в сетях передачи данных</b>		
<i>Лекции</i>		
	Лекция 3.6.1. Абонентское шифрование. Пакетное шифрование. Защита центра генерации ключей. Криptomаршрутизатор. Пакетный фильтр	3
	Лекция 3.6.2. Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протоколов	4
<b>Тема 3.7. Защита информации в электронных платежных системах</b>		
<i>Лекции</i>		
	Лекция 3.7.1. Принципы функционирования электронных платежных систем. Электронные пластиковые карты. Персональный идентификационный номер	4
	Лекция 3.7.2. Применение криптографических протоколов для обеспечения безопасности электронной коммерции.	2
<i>Практические занятия</i>		
	Практическое занятие 3.7.1. Применение аутентификации по одноразовым паролям. Реализация алгоритмов создания одноразовых паролей	2
<i>Самостоятельная работа обучающихся</i>		
	3.7.1. Законодательство в области криптографической защиты информации	2
<b>Тема 3.8. Компьютерная стеганография</b>		
<i>Лекции</i>		
	Лекция 3.8.1. Скрытая передача информации в компьютерных системах. Проблема аутентификации мультимедийной информации. Защита авторских прав.	4
	Лекция 3.8.2. Методы компьютерной стеганографии. Цифровые водяные знаки. Алгоритмы встраивания ЦВЗ	4
<i>Практические занятия</i>		
	Практическое занятие 3.8.1. Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ	2
	Практическое занятие 3.8.2. Реализация простейших стеганографических алгоритмов	2

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
<i>Самостоятельная работа обучающихся</i>		
	3.8.1. Программная реализация современных криптоалгоритмов	1
	3.8.2. Перспективные направления криптографии	1
<b>Консультации</b>		<u>6</u>
<b>Промежуточная аттестация в форме экзамена</b>		<u>6</u>
<b>Всего</b>		120

### 3 Материально-техническое и учебно-методическое обеспечение дисциплины (модуля)

#### 3.1 Специальные помещения для реализации программы

Наличия учебного кабинета «информационной безопасности, лаборатории информационных технологий».

##### Оборудование учебного кабинета:

- посадочные места по количеству обучающихся;
- рабочее место преподавателя;
- комплект учебно-наглядных пособий «Информационная безопасность»;
- электронное учебное пособие.

Технические средства обучения:

- компьютер с лицензионным программным обеспечением, мультимедийный диапроектор, интерактивная доска.

#### 3.2 Информационное обеспечение реализации программы

##### 3.2.1 Основная литература

1. Казарин, О. В. Программно-аппаратные средства защиты информации. защита программного обеспечения.: учебник и практикум для СПО / Казарин О. В., Забабурин А. С.. – Москва : Юрайт, 2021. – 312 с. – ISBN 978-5-534-13221-2. – URL:<https://urait.ru/book/programmno-apparatnye-sredstva-zaschity-informacii-zaschita-programmnogo-obespecheniya-476997>. – Текст : электронный.

##### 3.2.2. Дополнительная литература

1. Бабенко, Л. К. Криптографическая защита информации: симметричное шифрование.: учебное пособие для вузов / Бабенко Л. К., Ищукова Е. А.. – Москва : Юрайт, 2020. – 220 с. – ISBN 978-5-9916- 9244-1. – URL:<https://urait.ru/book/kriptograficheskaya-zaschita-informacii-simmetrichnoe-shifrovanie-452871>. – Текст : электронный.

2. Введение в теоретико-числовые методы криптографии : учебное пособие / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. — Санкт-Петербург : Лань, 2022. — 400 с. — ISBN 978-5-8114- 1116-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL:<https://e.lanbook.com/book/210746>. — Режим доступа: для авториз. пользователей.

3. Никифорова, Д. Ф. Криминалистические проблемы расследования преступлений, совершенных с использованием криптографических валют / Д. Ф. Никифорова ; Юридический факультет; Министерство сельского хозяйства Российской Федерации. – Краснодар : б.и., 2019. – 79 с. – URL:[http://biblioclub.ru/index.php?page=book\\_red&id=594174](http://biblioclub.ru/index.php?page=book_red&id=594174). – Текст : электронный.

4. Ермакова, А. Ю. Криптографические методы защиты информации : учебно-методическое пособие / А. Ю. Ермакова. — Москва : РГУ МИРЭА, 2021. — 172 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL:<https://e.lanbook.com/book/176563>. — Режим доступа: для авториз. пользователей.

##### 3.2.3 Методическая литература

1. Профессиональный цикл : методические материалы для обучающихся направления подготовки 10.02.05 "Обеспечение информационной безопасности автоматизированных систем" / Кузбасский государственный технический университет им. Т. Ф. Горбачева ; Кафедра информационной безопасности, составители: Е. В. Прокопенко, А. В. Медведев, А. Г. Киренберг. – Кемерово : КузГТУ, 2020. – 290 с. – URL:<http://library.kuzstu.ru/meto.php?n=9964>. – Текст : электронный.

##### 3.2.4 Интернет ресурсы

#### 1. ЭИОС КузГТУ:

- а) Электронная библиотека КузГТУ. – Текст: электронный // Научно-техническая библиотека Кузбасского государственного технического университета им. Т. Ф. Горбачева : сайт. – Кемерово, 2001 – . – URL: <https://elib.kuzstu.ru/>. – Текст: электронный.
- б) Портал.КузГТУ : Автоматизированная Информационная Система (АИС) : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: <https://portal.kuzstu.ru/>. – Режим доступа: для авториз. пользователей. – Текст: электронный.
- с) Электронное обучение : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: <https://el.kuzstu.ru/>. – Режим доступа: для авториз. пользователей КузГТУ. – Текст: электронный.
2. ФСТЭК России : Федеральная служба по техническому и экспортному контролю : официальный сайт / ФАУ «ГНИИИ ПТЗИ ФСТЭК России». – Москва, 2004 – . – URL: [www.fstec.ru](http://www.fstec.ru). – Текст: электронный.
3. SecurityLab.ru : информационный портал по безопасности : сайт. – Москва. – URL: <https://www.securitylab.ru/>. – Текст: электронный.
4. Департамент образования Вологодской области : официальный сайт. – Вологда. – URL: <http://depobr.gov35.ru/>. – Текст: электронный.
5. BIOMETRICS.RU : Российский биометрический портал : сайт. – Москва, 2000 – . – URL: [www.biometrics.ru](http://www.biometrics.ru). – Текст: электронный.
6. InformationSecurity/Информационная безопасность : сайт. – Москва. – URL: <http://www.itsec.ru>. – Текст: электронный.
7. eLIBRARY.RU : научная электронная библиотека : сайт. – Москва, 2000 – . – URL: <https://elibrary.ru>. – Режим доступа: для зарегистрир. пользователей. – Текст: электронный.
8. Гарант. ру : информационно-правовой портал : сайт. – Москва, 1990 – . – URL: <https://www.garant.ru/>. – Текст: электронный.
9. КонсультантПлюс : компьютерная справочно-правовая система : сайт. – Москва, 1992 – . – URL: [www.consultant.ru](http://www.consultant.ru). – Текст: электронный.
10. Единое окно доступа к образовательным ресурсам : информационная система : сайт / ФГАУ ГНИИ ИТТ «Информика» . – Москва, 2005 – . – URL: <http://window.edu.ru/>. – Текст: электронный.
11. Российское образование. Федеральный образовательный портал : сайт / ФГАОУ ДПО ЦРГОП и ИТ. – Москва, 2002 – . – URL: [www.edu.ru](http://www.edu.ru). – Текст: электронный.

#### **4. Организация самостоятельной работы обучающихся**

Самостоятельная работа обучающихся осуществляется в объеме, установленном в разделе 2 настоящей программы дисциплины (модуля).

Для самостоятельной работы обучающихся предусмотрены специальные помещения, оснащенные компьютерной техникой с возможностью подключения к информационно-телекоммуникационной сети "Интернет" с обеспечением доступа в электронную информационно-образовательную среду КузГТУ.

#### **6. Иные сведения и (или) материалы**

1. Образовательный процесс осуществляется с использованием как традиционных, так и современных интерактивных технологий. При контактной работе педагогического работника с обучающимися применяются следующие элементы интерактивных технологий:

- совместный разбор проблемных ситуаций;

- совместное выявление причинно-следственных связей вещей и событий, происходящих в повседневной жизни, и их сопоставление с учебным материалом.

2. Проведение групповых и индивидуальных консультаций осуществляется в соответствии с расписанием консультаций по темам, заявленным в рабочей программе дисциплины, в период освоения дисциплины и перед промежуточной аттестацией с учетом результатов текущего контроля.