Министерство науки и высшего образования Российской Федерации

федеральное государственное бюджетное образовательное учреждение
высшего образования
«Курганский государственный университет»
(КГУ)
Кафедра «Безопасность информационных и автоматизированных систем»

УТВЕРЖДАЮ
Первый проректор
_____ /Т.Р. Змызгова /
«31» августа 2023 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

(наименование дисциплины)

образовательной программы высшего образования –

программы специалитета

«**10.05.03 – Информационная безопасность автоматизированных систем**»

Специализация (Специализация №5):

«**Безопасность открытых информационных систем**»

Форма обучения: очная

Курган 2023

ПРИЛОЖЕНИЕ 1

Аннотация к рабочей программе дисциплины

«Методы и средства криптографической защиты информации»

образовательной программы высшего образования –
программы специалитета
10.05.03 - Информационная безопасность автоматизированных систем
Специализация: Безопасность открытых информационных систем

Форма обучения: очная

Трудоемкость дисциплины: 5 з.е. (180 академических часа)
Семестр: 4 (очная форма обучения)
Форма промежуточной аттестации: экзамен
Содержание дисциплины. Основные разделы.

Криптология: криптография и криптоанализ. Криптография и проблемы безопасности информации: конфиденциальность, целостность, аутентификация, невозможность отказа сторон от авторства. Основные понятия криптографии: шифр, ключ, криптосистема, шифрование, дешифрование и др. Правило Керкхоффса. Криптосистема. Структура криптосистемы. Криптостойкость. Классификация методов криптографической защиты информации. Перестановочные шифры. Подстановочные шифры. Потоковые шифры. Блочные шифры. Симметричное и ассиметричное шифрование. Симметричные криптоалгоритмы. Ассиметричные криптоалгоритмы. Принципы построения, описания и анализа криптографических алгоритмов. Сеть Фейштеля. Криптоалгоритмы на основе сети Фейстеля. Криптоалгоритмы на основе подстановочно-перестановочных сетей (SP-сети). Криптоалгоритмы со структурой "квадрат". ПО для шифрования данных. Принципы построения и криптоанализ симметричных и ассиметричных систем защиты информации. Стандадарты криптографиеческой защиты информации. Хэш-функции. Электронная цифровая подпись или цифровая подпись. Алгоритмы цифровой подписи. Криптографические протоколы.