

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

(должность)



(Handwritten signature)
(подпись, Ф.И.О.)

/Т.Р. Змызгова/

» *(Handwritten signature)* 2021 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
ТЕОРЕТИЧЕСКИЕ ОСНОВЫ КРИПТОЛОГИИ
(наименование дисциплины)

образовательной программы высшего образования –
программы специалитета

«10.05.03 - Информационная безопасность автоматизированных систем»
Специализация (Специализация № 5): **«"Безопасность открытых информаци-
онных систем"»**

Форма обучения: очная

Курган 2021

Аннотация к рабочей программе дисциплины
«Теоретические основы криптологии»

образовательной программы высшего образования –
программы специалитета

10.05.03 - Информационная безопасность автоматизированных систем
Специализация: Безопасность открытых информационных систем
Форма обучения: очная

Трудоемкость дисциплины: 3 з.е. (108 академических часа).

Семестр: 5 (очная форма обучения).

Форма промежуточной аттестации: дифференцированный зачет.

Содержание дисциплины. Основные разделы.

Криптология: криптография и криптоанализ. Криптостойкость. Криптоатака. Математические основы криптологии и криптографии. Классификация методов криптографической защиты информации. Принципы построения и анализа криптографических алгоритмов. Статистический криптоанализ. Алгебраический криптоанализ. Дифференциальный (или разностный) криптоанализ. Линейный криптоанализ.