Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Саратовский государственный технический университет
имени Гагарина Ю.А.»

Кафедра «Информационная безопасность автоматизированных систем»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ

по дисциплине С.1.1.25 «Криптографические методы защиты информации»

специальности подготовки
10.05.03 «Информационная безопасность автоматизированных систем»
Специализация «Создание автоматизированных систем в защищенном исполнении»

форма обучения – очная
курс – 3
семестр – 6
зачетных единиц – 6
часов в неделю – 5
всего часов – 216,
в том числе:
лекции – 32
практические занятия – 48
самостоятельная работа – 136
экзамен – 6 семестр

1. Цели и задачи дисциплины

Цель преподавания дисциплины:
Целью курса «Криптографические методы защиты информации» является обучение студентов основам криптографического сокрытия информации.

Задачи изучения дисциплины:
Знакомство и практическое освоение криптографическими средствами защиты информации.

2. Место дисциплины в структуре ООП ВО

Дисциплина «Криптографические методы защиты информации» является дисциплиной базовой части цикла дисциплин ФГОС ВО по специальности 10.05.03 "Информационная безопасность автоматизированных систем".
Дисциплина «Криптографические методы защиты информации» базируется на знаниях, полученных в рамках изучения следующих дисциплин: «Информатика», «Дискретная математика», «Математика».

3. Требования к результатам освоения дисциплины

Изучение дисциплины направлено на формирование следующих компетенций:
ОПК-2 способностью применять соответствующий математический аппарат для решения профессиональных задач;
ПК-14 способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности.

Студент должен знать:

– основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в компьютерных сетях;
– основные задачи и понятия криптографии;
- требования к шифрам и основные характеристики шифров;
- типовые поточные и блочные шифры;
- частотные характеристики открытых текстов и способы их применения к анализу простейших шифров замены и перестановки;
- типовые шифры с открытыми ключами;
- модели шифров и математические методы их исследования;
- основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические);
— основные криптографические методы, алгоритмы, протоколы используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах;
- основные методы управления информационной безопасностью;
- основные нормативные правовые документы в области криптографической защиты информации.

Студент должен уметь:

– эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах;
– применять нормативные правовые документы в области криптографической защиты информации на практике;
– применять математические методы исследования моделей шифров.

Студент должен владеть:

– - криптографической терминологией;
– - навыками использования ЭВМ в анализе простейших шифров;
– - навыками математического моделирования в криптографии;
– - навыками разработки документации в области криптографической защиты информации;
– - навыками использования типовых криптографических алгоритмов.