

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 Б.1.1.16 «Криптографические методы защиты информации»

направления подготовки
10.03.01 "Информационная безопасность"
Профиль «Безопасность автоматизированных систем»

форма обучения – очная
курс – 2
семестр – 4
зачетных единиц – 4
часов в неделю – 4
всего часов – 144 ,
в том числе:
лекции – 32
практические занятия – 32
самостоятельная работа – 80
экзамен – 4 семестр

1. Цели и задачи 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 направлению 10.03.01 "Информационная безопасность" по профилю "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-1 Способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации.

Студент должен знать:

основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в компьютерных сетях;

модели шифров и математические методы их исследования;

принципы построения криптографических алгоритмов;

криптографические стандарты и их использование в информационных системах;

основные нормативные правовые документы в области криптографической защиты информации;

аппаратные средства вычислительной техники;

технические средства защиты информации;

принципы организации информационных систем в соответствии с требованиями по защите информации;

основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах.

Студент должен уметь:

эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах;

применять математические методы исследования моделей шифров;

использовать программные и аппаратные средства персонального компьютера;

осуществлять поиск информации по профилю деятельности в различных источниках, в том числе в глобальных компьютерных системах;

применять нормативные правовые документы в области криптографической защиты информации на практике;

анализировать и оценивать угрозы информационной безопасности объекта;
осуществлять меры противодействия нарушениям безопасности с использованием различных программных и аппаратных средств защиты;
пользоваться сетевыми средствами для осуществления поиска, изучения, обобщения и систематизации научно-технической информации, нормативных и методических материалов в области криптографической защиты информации.

Студент должен владеть:

криптографической терминологией;
навыками использования типовых криптографических алгоритмов;
навыками использования ЭВМ в анализе простейших шифров;
навыками математического моделирования в криптографии;
навыками поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов, СУБД и т.п.);
навыками разработки документации в области криптографической защиты информации;
методами и средствами выявления угроз безопасности автоматизированным системам;
методами технической защиты информации.