Аннотация рабочей программы дисциплины
ТЕОРИЯ И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ
для направления подготовки
01.03.04 Прикладная математика
Квалификация (степень) выпускника
бакалавр

Общая трудоемкость дисциплины, изучаемой в 6 семестре, составляет 3 зачетных единиц (108 академических часа). По дисциплине предусмотрен зачет.

(форма контроля зачет)

Цели и задачи освоения дисциплины *(из раздела 1 рабочей программы)*

Дисциплина «Теория и методы защиты информации» (ТМЗИ) относится к учебному вариативному циклу и имеет своей целью изучение основных закономерностей криптозащиты информации в системах связи. Она должна способствовать развитию творческих способностей студентов прикладной математики к решению практических задач в области защиты информации от несанкционированного её подмены и использования.

Задача дисциплины ТМЗИ состоит в том, чтобы ознакомить студентов с основами защиты информации, а также с основными методами и средствами современной криптографии для решения проблем, возникающих при обработке, хранении и передаче информации.

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО по данному направлению:

а) общекультурных (ОК):

способностью к самоорганизации и самообразованию (ОК-7);

б) общепрофессиональных (ОПК):

готовностью к самостоятельной работе (ОПК-1);

в) профессиональных (ПК):

владеть основными методами защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий (ПК-8);

готовностью применять математический аппарат для решения поставленных задач, способностью применить соответствующую процессу математическую модель и проверить ее адекватность, провести анализ результатов моделирования, принять решение на основе полученных результатов (ПК-10).

В результате освоения дисциплины обучающийся должен:

Знать:

– основные математические методы и алгоритмы защиты информации путем шифрования, расшифрования и дешифрования сообщений (ПК-8),

– электронной (цифровой) подписи в телекоммуникационных системах (ПК-8, ПК-10),

– принципы работы, структурные схемы, протоколы и способы программирования криптосистем и систем электронной подписи, (ОК-7, ПК-10),

Уметь:

– пользоваться методами теории чисел (ПК-10),

– составлять протоколы шифрования и расшифрования сообщений (ОПК-1, ПК-10),

– оценивать теоретическую и практическую стойкость шифров (ПК-8).

Владеть

– приемами проектирования типовых алгоритмов криптозащиты и криптоанализа сообщений (ПК-10).

– методами оценки криптостойкости систем защиты информации (ПК-8).

Основные разделы дисциплины: *(из раздела 5.1 рабочей программы)*

1 Введение в криптографические системы защиты информации (КСЗИ)
2 Теоретико-информационные основы криптозащиты сообщений
3 Симметричные КСЗИ
4 Асимметричные КСЗИ
5 Управление криптографическими ключами
6 Электронные (цифровые) подписи
7 Имитозащита информации

Разработчик программы:
профессор, к.т.н. (доцент), В.Г. Санников

Заведующий кафедрой ОТС А.С. Аджемов