Приложение 1

Аннотация рабочей программы

Дисциплина «Криптографические методы защиты информации» относится к базовой части профессиональных дисциплин и предназначена наряду с другими дисциплинами для осуществления профессиональной подготовки студентов в области защиты информации.

Необходимыми условиями для освоения дисциплины являются знание основ математики, дискретной математики, теории вероятностей и математической статистики, теории информации, модулярной арифметики, теории множеств, математическая логика и теория алгоритмов, основы вычислительной техники и программирования.

Учебная дисциплина «Криптографические методы защиты информации» входит в состав блока Б3.Б.3 и относится к базовому циклу профессиональных дисциплин подготовки специалистов по направлению 090900 «Информационная безопасность» по профилю «Комплексная защита объектов информации».

Необходимыми условиями для освоения дисциплины являются знание основ математики, дискретной математики, теории вероятностей и математической статистики, теории информации, модулярной арифметики, теории множеств, математическая логика и теория алгоритмов, основы вычислительной техники и программирования.

Изучаемый в курсе криптографические алгоритмы, а также приобретаемые навыки решения прикладных задач используются при изучении ряда общих и специальных дисциплин, таких как «Криптографические протоколы».

Целями освоения дисциплины « Криптографические методы защиты информации» является формирование профессиональных компетенций, необходимых для осуществления проектно-конструкторской, научно-исследовательской, производственно-технологической, организационно-управленческой, экспертно-аналитической деятельности:

способностью выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации (ПК-11);

способностью применять программные средства системного, прикладного и специального назначения (ПК-15);

способностью использовать инструментальные средства и системы программирования для решения профессиональных задач (ПК-16);

способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности (ПК-19);

изложение основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике.

Задачи изучения дисциплины являются:

получение знаний по основным понятиям криптографии; моделям шифров и математическим методам их исследования; требованиям, предъявляемым к шифрам и основным характеристикам шифров; по основополагающим принципам защиты информации на основе криптографических методов; криптографическим стандартам и их использовании в информационных системах;

приобретение умений по реализации криптографических методов на практике;

овладение навыками владения криптографической терминологией; использования типовых криптографических алгоритмов; использование ПЭВМ в анализе простейших шифров; математического моделирования в криптографии;

Требования к уровню освоения содержания дисциплины.

В результате изучения дисциплины студент должен приобрести:

-**знания** о основных задачах и понятиях криптографии; требованиях к шифрам и основных характеристиках шифров; моделях шифров и математических методах их исследования; принципах построения криптографических алгоритмов, криптографических стандартах и их использовании в информационных системах;

- умения применять криптографические алгоритмы на практике; применять отечественные и зарубежные стандарты в области криптографических методов компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;
- навыки владения криптографической терминологией; использования типовых криптографических алгоритмов; использования математического моделирования в криптографии;- средствами обеспечения информационной безопасности**,** определения видов и форм информаций подверженных угрозам и возможных методов и путей устранения этих угроз.

Содержание дисциплины рассматриваются криптографические алгоритмы положенные в основу криптографических протоколов без которых невозможно было бы создать современные криптографические методы и средства защиты информации в компьютерных системах и сетях.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, практические занятия, самостоятельная работа студента, консультации**.**

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тренировочных тестов; рубежный контроль контрольных тестов, и промежуточный контроль в форме экзаменов.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единиц, _108_ часов. Программой дисциплины предусмотрены лекционные: 36 часов, лабораторные занятия: 18 часов, самостоятельная работа студента: 54 часа.