Аннотация рабочей программы дисциплины

«Основы информационной безопасности»

Направление подготовки: 11.03.02 - Инфокоммуникационные технологии и системы связи
Профили подготовки: Программно-защищенные инфокоммуникации
Квалификация (степень) выпускника: Академический бакалавр

Общая трудоемкость дисциплины, изучаемой в 5-ом семестре, составляет 3 зачетных единиц (108 часов). По дисциплине предусмотрен зачет.

Цели и задачи освоения дисциплины

Целями освоения дисциплины «Основы информационной безопасности» являются:

- развитие творческих подходов при решении сложных научно-технических задач, связанных с обеспечением информационной безопасности государства и его информационной инфраструктуры;
- развитие профессиональной культуры, формирование научного мировоззрения и развитие системного мышления;
- привитие стремления к поиску оптимальных, простых и надежных решений;
- расширение кругозора.

Задачи освоения дисциплины «Основы информационной безопасности» – дать знания по вопросам:

- обеспечения информационной безопасности государства;
- методологии создания систем защиты информации;
- процессов сбора, передачи и накопления информации;
- методов и средств ведения информационных войн;
- оценки защищенности и обеспечения информационной безопасности компьютерных систем.

Требования к результатам освоения дисциплины

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

- готовностью изучать научно-техническую информацию, отечественный и зарубежный опыт по тематике исследования (ПК-16);
- способностью применять современные теоретические и экспериментальные методы исследования с целью создания новых перспективных средств электросвязи и информатики (ПК-17);
- способностью организовывать и проводить экспериментальные испытания с целью оценки соответствия требованиям технических регламентов, международных и национальных стандартов и иных нормативных документов (ПК-18);

Основные разделы дисциплины

1. Информационная безопасность в системе национальной безопасности Российской Федерации;
2. Информационная война, методы и средства ее ведения;
3. Критерии защищенности компьютерных систем;

4. Защита информации, обрабатываемой в автоматизированных системах, от технических разведок;
5. Защита АС и СВТ от внешнего электромагнитного воздействия;
6. Технические средства защиты сетей и систем связи от утечки конфиденциальной информации.

Разработчик(и) программы:
Д.т.н., профессор кафедры ИБиА Шелухин О.И.

Заведующий кафедрой ИБиА,
д.т.н., профессор Шелухин О.И.

Центр документационного обеспечения