

Аннотация рабочей программы дисциплины

Инженерно-техническая защита объектов инфокоммуникаций

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 7-ом семестре, составляет 4 зачетных единиц (144 часов). По дисциплине предусмотрен зачет в 7-ом семестре.

Цели и задачи освоения дисциплины

Целью освоения дисциплины является изучение студентами принципов построения и особенностям функционирования средств инженерно-технической защиты объектов инфокоммуникаций и включает в себя как методы и средства инженерно-технической защиты информации так и технические средства охраны объектов и помещений. В результате изучения дисциплины у студентов должны сформироваться знания, умения и навыки, позволяющие проводить самостоятельный анализ физических процессов, происходящих в инженерно-технических средствах защиты объектов, как изучаемых в настоящей дисциплине, так и находящихся за ее рамками.

В результате изучения настоящей дисциплины студенты должны получить знания, имеющие не только самостоятельное значение, но и обеспечивающие базовую подготовку для усвоения ряда последующих дисциплин в области программно-защищенных инфокоммуникаций.

Задачи освоения дисциплины:

- формирование знаний, умений и навыков, позволяющих проводить самостоятельный анализ средств и методов технической защиты объектов инфокоммуникаций, как изучаемых в настоящей дисциплине, так и находящихся за ее рамками;
- обеспечение базовой подготовки для усвоения ряда последующих дисциплин в области информационной безопасности.

Требования к результатам освоения дисциплины

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

профессиональных компетенций (ПК):

- 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);
- готовностью к организации работ по практическому использованию и внедрению результатов исследований (ПК-19);

Основные разделы дисциплины

1. Введение
2. Объекты информационной защиты
3. Технические средства охраны объектов инфокоммуникаций

4. Способы и средства добывания информации техническими средствами.
Технические каналы утечки информации
5. Методология проектирования и моделирования инженерно-технической защиты объектов инфокоммуникаций.

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



Шелухин О.И.

Заведующий кафедрой ИБиА,
д.т.н., профессор



Шелухин О.И.