

Аннотация к рабочей программе по учебной дисциплине «ФИЗИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ»

1. Цель и задачи учебной дисциплины:

Целью изучения дисциплины «Физические основы защиты информации» является подготовка студентов к формированию научно-технических задач, определяющих современное развитие в области защиты информации от утечек по техническим каналам, обусловленных электрическими сигналами, физическими информационными полями рассеивания и их наводками.

Достижение поставленной цели осуществляется путём решения следующих задач:

а) сформировать у студента представление о:

- программах и методиках испытаний технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок;
- испытаниях технических средств защиты информации от утечки за счет побочных электромагнитных излучений;
- методах оценки и разрушения каналов утечки информации, маскирования сигналов и их искажения с целью скрытия факта, места, времени и содержания;

б) научить студента:

- проводить испытания технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок на соответствие требованиям безопасности информации и техническим условиям;
- осуществлять защиту информации от несанкционированных действий;
- осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями;
- проводить отдельные работы по физической защите линий связи информационно-телекоммуникационных систем и сетей;
- использовать техническую и справочную литературу;
- использовать информационные технологии для поиска и решения профессионально значимых задач.
- пользоваться технической и справочной литературой;
- использовать наиболее эффективные и оптимальные способы решения поставленных задач.

2. Требования к результатам освоения дисциплины

В результате освоения дисциплины у обучаемого должны быть сформированы следующие компетенции:

ОК-1: выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам;

ОК-2: осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности;

ПК-2.3: осуществлять защиту информации от несанкционированных действий;

ПК-3.3: осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями;

ПК-3.4: проводить отдельные работы по физической защите линий связи информационно-телекоммуникационных систем и сетей.

В результате изучения дисциплины студент

должен: - **знать:**

- программы и методики испытаний технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок на соответствие требованиям безопасности информации и техническим условиям;

- методы оценки и разрушения каналов утечки информации, маскирования сигналов и их искажения;

- способы защиты информации от несанкционированных действий;

- **уметь:**

- разрабатывать программы и методики испытаний технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок на соответствие требованиям безопасности информации и техническим условиям;

- проводить испытания технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок на соответствие требованиям безопасности информации и техническим условиям -демонстрировать ответственность за принятые решения;

- обосновывать результаты собственной работы;

- взаимодействовать с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик;

- обосновывать анализ работы членов команды (подчиненных)

- проводить отдельные работы по физической защите линий связи информационно-телекоммуникационных систем и сетей.

3. Содержание дисциплины. Основные разделы.

1. Основные понятия и определения физических основ защиты информации
2. Методы оценки и разрушения каналов утечки информации