МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

САМАРСКИЙ ГОСУДАРСТВЕННЫЙ ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ

Институт систем управления

Кафедра прикладной информатики и информационной безопасности

АННОТАЦИЯ

по дисциплине

«Инженерно-техническая защита информации»

направление подготовки 10.03.01 Информационная безопасность

профиль «Организация и технология защиты информации»

очной формы обучения

Соответствует РПД

УМУ СГЭУ

Зав. кафедрой

/Абросимов А.Г./

Самара 2015 г.

1. Цели и задачи дисциплины

Цель дисциплины «Инженерно-техническая защита информации» - обучить студентов основным положениям современной инженерно-технической защиты информации, принципам инженерно-технической защиты источников, носителей и получателей информации, а также принципам построения технических средств охраны объектов,

Задачами изучения дисциплины являются приобретение знаний об опасных сигналах, демаскирующих признаках объектов защиты, возможностях технических каналов утечки информации, получение сведений о состоянии и перспективах их развития, приобретение навыков по выявлению угроз безопасности информации и определению мер защиты объектов информатизации.

2. Место дисциплины в структуре ООП

Дисциплина «Инженерно-техническая защита информации» относится к циклу профессиональных дисциплин по направлению подготовки 10.03.01 "Информационная безопасность" профиль "Организация и технология защиты информации. Для изучения дисциплины необходимы знания, умения и компетенции студента, которые были получены при изучении дисциплин: аппаратные средства вычислительной техники, программно-аппаратные средства защиты информации, криптографические методы защиты информации, сети и системы передачи информации

Данная дисциплина является базовой для изучения студентами обязательных дисциплин: комплексная система защиты информации на предприятии, в разработке и внедрении ВКР

3. Требования к уровню освоения содержания дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

профессиональных (ПК):

ПК-15	способностью применять программные средства системного, прикладного и специального назначения
ПК-18	способностью собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности
ПК-26	способностью формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью

В результате изучения дисциплины студент должен:

Знать:

- основные источники и носители информации различных видов;
- демаскирующие признаки объектов защиты;
- угрозы безопасности информации;
- возможности технических каналов утечки информации и методы их оценки;
- методы и способы защиты информации;
- показатели эффективности защиты и методы их оценки.

Уметь:

- описывать (моделировать) объекты защиты,
- выявлять и оценивать угрозы безопасности информации на конкретных объектах;
- определять рациональные меры защиты на объектах информатизации и оценивать их эффективность
- контролировать эффективность мер инженерно-технической защиты информации

Приобрести навыки:

- по определению технических каналов утечки информации на различных объектах;
- по выбору различных датчиков и систем для обнаружения каналов утечки;
- по расчетам основных параметров системы защиты.

4. Объем дисциплины и виды учебной работы

Вид учебной работы	**Всего часов/ зачетных единиц УП 2012г**	**Всего часов/ зачетных единиц УП 2013г**	**Всего часов/ зачетных единиц УП 2014,2015г.**
Аудиторные занятия	126/3,5	72/2	72/2
В том числе:			
Лекции	54/1,5	36/1	36/1
Практические занятия (ПЗ)			
Лабораторные работы (ЛР)	72/2	36/1	36/1
Самостоятельная работа (всего)	90/2,5	144/4	36/1
Курсовой проект (работа)	курсов.раб.	курсов.раб.	курсов.раб.
Расчетно-графические работы			
Реферат			
Другие виды самостоятельной работы			
Вид промежуточной аттестации (зачет, экзамен)	Зачет- 5 сем. Экзамен -6 сем. 36/1	Зачет- 5 сем. Экзамен -6 сем. 36/1	Экзамен - 6 сем. 36/1
Общая трудоемкость	252 /7	252 /7	144 /4