Аннотация к рабочей программе дисциплины

«Техническая защита информации»

Курс учебной дисциплины «Техническая защита информации» предназначен для обучения студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав базовых дисциплин учебного плана Б1.Б.12.03.

Общая трудоемкость освоения дисциплины составляет 144 часа (4 з.е.). Учебным планом предусмотрены лекционные занятия (36 час.), лабораторные работы (36 час.), самостоятельная работа (36 час., в том числе 36 час. на подготовку к экзамену). Дисциплина реализуется на 5 курсе, в 9 семестре. Форма контроля по дисциплине – экзамен.

Дисциплина «Техническая защита информации» логически и содержательно связана с такими курсами, как «Операционные системы», «Основы информационной безопасности», «Аппаратные средства вычислительной техники».

Курс лекций построен на пошаговом повествовании от технических каналов утечки информации и средствам технической защиты информации.

Цель дисциплины: раскрыть природу формирования технических каналов утечки информации, сформировать представление о проблемах защиты технических каналов утечки информации, выработать умения и навыки по определению потенциальных каналов утечки информации на объектах информатизации, по выработке рекомендаций по защите конкретного канала утечки, ознакомить с процессом сертификации средств защиты и мероприятиями аттестации объектов информатизации на соответствие требованиям безопасности информации.

Задачи дисциплины:

- привести анализ физических процессов приводящих к появлению опасных сигналов демаскирующих защищаемые объекты;

- дать физические основы процессов образования технических каналов

утечки информации;

- дать физическое обоснование технических характеристик каналов утечки информации;

- изложить концепцию и методы инженерно-технической защиты информации;

- дать представление о формировании базы нормативных документов по противодействию технической и видам контроля эффективности защиты информации.

Для успешного изучения дисциплины «Техническая защита информации» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-4);
- способность использовать нормативные правовые акты в своей профессиональной деятельности (ОПК-5);

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные/ профессиональные компетенции (элементы компетенций).

Код и формулировка компетенции	**Этапы формирования компетенции**	
ОПК-9 – способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации	Знать	основные виды политик управления доступом и информационными потоками в компьютерных системах; основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков
	Уметь	разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем; разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом

		и информационными потоками
	Владеть	навыками разработки моделей угроз и моделей нарушителя
ПК-19 – способность производить проверки технического состояния и профилактические осмотры технических средств защиты информации	Знать	принципы работы оборудования по защите информации
	Уметь	проводить проверку технического состояния оборудования по защите информации
	Владеть	навыками настройки оборудования по защите информации

Для формирования вышеуказанных компетенций в рамках дисциплины «Техническая защита информации» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: собеседование (ОУ-1), коллоквиум (ОУ-2), лабораторные работы (ПР-6), конспект (ПР-7).