

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Смирнов Сергей Николаевич
Должность: врио ректора
Дата подписания: 16.10.2023 14:57:08
Уникальный программный ключ:
69e375c64f7e975d4e8830e7b4f1cc2ad12b735f08

Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Тверской государственный университет»



Утверждаю:

Руководитель ООП:

 Н.А. Семькина

« 9 » 06 2023 г.

Рабочая программа дисциплины (с аннотацией)

Техническая защита информации

Специальность

10.05.01 Компьютерная безопасность

Специализация

Математические методы защиты информации

Для студентов V курса очной формы обучения

Составитель:

к.ф.м.н., доцент  Н.А. Семькина

Тверь 2023

I. Аннотация

1. Наименование дисциплины (или модуля) в соответствии с учебным планом

Техническая защита информации.

2. Цель и задачи дисциплины (или модуля)

Целью дисциплины является: формирование у студентов знаний по основам инженерно-технической защиты информации, а также навыков и умения в применении знаний для конкретных условий; развитие системного мышления, необходимого для решения задач инженерно-технической защиты информации с учетом требований системного подхода.

Задачи дисциплины:

- изучение концепции инженерно-технической защиты информации;
- изучение теоретических основ инженерно-технической защиты информации;
- изучение физических основ инженерно-технической защиты информации;
- изучение технических средств добывания и защиты информации;
- изучение организационных основ инженерно-технической защиты информации;
- изучение методического обеспечения инженерно-технической защиты информации.

3. Место дисциплины (или модуля) в структуре ООП

Дисциплина «Техническая защита информации» относится к числу дисциплин базовой части профессионального цикла.

Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин:

«Информатика» – работа с программными средствами общего назначения;

«Аппаратные средства вычислительной техники» – знание архитектуры основных типов современных компьютерных систем;

«Операционные системы» – знание принципов построения современных операционных систем и особенностей их применения, владение навыками конфигурирования и администрирования операционных систем.

4. Объем дисциплины (или модуля):

3 зачетных единиц, 108 академических часов, **в том числе**

контактная работа: лекции 15 часов, практические занятия 30 часов, самостоятельная работа: 63 часа.

5. Перечень планируемых результатов обучения по дисциплине (или модулю), соотнесенных с планируемыми результатами освоения образовательной программы

<p>Планируемые результаты освоения образовательной программы (формируемые компетенции)</p>	<p>Планируемые результаты обучения по дисциплине (или модулю)</p>
<p>ОПК-3 – способностью понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и в иных источниках информации</p>	<p>Владеть: навыками анализа информации, навыками использования нормативных документов по противодействию технической разведке. Уметь: осуществлять подбор, изучение и обобщение научно-технической информации по способам и средствам технической защиты информации. Знать: нормативные документы по противодействию технической разведке.</p>
<p>ПК-9. способностью участвовать в проведении экспериментально-исследовательских работ при аттестации объектов с учетом требований к уровню</p>	<p>Владеть: методами и средствами технической защиты информации; методами защиты информации от несанкционированного доступа и специальных программных воздействий на нее. Уметь: проводить аттестационные испытания объектов вычислительной техники на соответствие требованиям по защите информации, пользоваться нормативными документами по противодействию технической разведке; оценивать качество готового</p>

защищенности компьютерной системы	программного обеспечения. Знать: средства и методы предотвращения и обнаружения вторжений; технические каналы утечки информации; возможности технических средств перехвата информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации.
ПК-19. способностью производить проверки технического состояния и профилактические осмотры технических средств защиты информации	Владеть: методами и средствами технической защиты информации, методами расчета и инструментального контроля показателей технической защиты информации. Уметь: пользоваться нормативными документами по противодействию технической разведке; оценивать качество готового программного обеспечения. Знать: технические каналы утечки информации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации.
ПК-20. способностью выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций	Владеть: способностью производить проверку технического состояния и профилактические осмотры оборудования по защите информации. Уметь: выполнять работы по приему, настройке, регулировке, освоению и восстановлению работоспособности оборудования защиты информации. Знать: средства и методы предотвращения и обнаружения вторжений, методы восстановления работоспособности средств защиты информации при возникновении нештатных ситуаций.

6. Форма промежуточной аттестации зачет

7. Язык преподавания русский.