

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Смирнов Сергей Николаевич
Должность: врио ректора
Дата подписания: 17.10.2023 14:21:13
Уникальный программный ключ:
69e375c64f7e975d4e8830e7b4fcc2ad1bf35f08

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

Утверждаю:
Руководитель ООП
Н.А. Семькина


« 4 » 09 2023 г.


Рабочая программа дисциплины (с аннотацией)

Основы построения защищенных компьютерных сетей

Специальность

10.05.01 Компьютерная безопасность

Специализация

«Математические методы защиты информации»

Для студентов очной формы обучения

СПЕЦИАЛИТЕТ

Для студентов 5 курса ОФО

Составитель:
Семькина Н. А.



I. Аннотация

1. Цель и задачи дисциплины

Целью освоения дисциплины - теоретическая и практическая подготовка специалистов к деятельности, связанной с построением защищенных сетевых автоматизированных систем, а также обучение принципам и методам защиты информации в компьютерных сетях.

Задачами освоения дисциплины являются:

- изучение типовых угроз безопасности в компьютерных сетях;
 - изучение криптографических и программно-аппаратных методов обеспечения информационной безопасности в компьютерных сетях;
 - приобретение навыков настройки и эксплуатации средств обеспечения безопасности в компьютерных сетях;
 - овладение средствами и методами проектирования и построения защищенных сетевых автоматизированных систем;
- овладение средствами и методами выявления и нейтрализации попыток нарушения безопасности в компьютерных сетях.

2. Место дисциплины в структуре ООП

Данная дисциплина входит в обязательную часть учебного плана, связана с другими дисциплинами образовательной программы: «Основы информационной безопасности», «Компьютерные сети», «Операционные системы», «Защита в операционных системах».

Дисциплины, для которых освоение данной дисциплины необходимо как предшествующее: «Научно-исследовательская работа», «Проектно-технологическая практика», «Преддипломная практика».

3. Объем дисциплины: 5 зачетные единицы, 180 академических часов, в том числе:

контактная аудиторная работа: лекции – 34 часов, в т.ч. практическая подготовка – 0 часов;

лабораторные занятия – 34 часов, в т.ч. практическая подготовка – 4 часа;

самостоятельная работа: 112 часа, в том числе контроль 27 часов.

4. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Планируемые результаты освоения образовательной программы (формируемые компетенции)	Планируемые результаты обучения по дисциплине
ОПК-8. Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей	ОПК-8.4 Применяет методики анализа сетевого трафика

<p>ОПК-10 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности</p>	<p>ОПК-10.5 Использует основные протоколы идентификации и аутентификации абонентов сети</p>
<p>ОПК-11. Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации</p>	<p>ОПК-11.1. Использует основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков</p>
<p>ОПК-15 Способен администрировать компьютерные сети и контролировать корректность их функционирования</p>	<p>ОПК-15.1 Осуществляет проектирование и оптимизацию функционирования компьютерных сетей</p> <p>ОПК-15.2 Работает с сетевым оборудованием и сетевым программным обеспечением</p>
<p>ОПК-16. Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях</p>	<p>ОПК-16.1. Применяет защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях</p> <p>ОПК-16.2. Осуществляет меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты</p>

5. Форма промежуточной аттестации и семестр прохождения – экзамен в 10 семестре.

6. Язык преподавания русский.