Министерство науки и высшего образования Российской Федерации

ФГБОУ ВО «Тверской государственный университет»

Утверждаю:

Руководитель ООП:

_____ Н.А. Семыкина

«_9_» _06_ 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 V курса очной формы обучения

Составитель:

к.ф.-м.н., доцент _____ Н.А. Семыкина

Тверь 2023

I. Аннотация

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

Основы построения защищенных компьютерных сетей

2. Цель и задачи дисциплины (или модуля)

Целью изучения дисциплины «Основы построения защищенных компьютерных сетей» является 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.

Задачи дисциплины:

- 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.

3. Место дисциплины (или модуля) в структуре ООП

Дисциплина «Основы построения защищенных компьютерных сетей» относится к числу дисциплин базовой части ООП.

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

«Информатика» – знание основных понятий информатики;

«Языки программирования» – знание языков программирования высокого уровня и языка ассемблера персонального компьютера, владение навыками разработки, документирования, тестирования и отладки программ;

«Основы информационной безопасности» – знание основных средств и способов обеспечения информационной безопасности, принципов построения систем защиты информации, владение профессиональной терминологией в области информационной безопасности;

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

«Защита в операционных системах» – знание защитных механизмов и средств обеспечения безопасности операционных систем, умение формулировать и настраивать политику безопасности основных операционных систем;

«Защита программ и данных» – знание основных средств и методов анализа программных реализаций, владение навыками анализа программных реализаций.

4. Объем дисциплины (или модуля):

3 зачетные единицы, 108 академических часов, **в том числе**

контактная работа: лекции 15 часов, практические занятия 30 часов, лабораторные работы 0 часов, **самостоятельная работа:** 18 часов, **контроль**: 45 часов.

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

Планируемые результаты освоения образовательной программы (формируемые компетенции)	**Планируемые результаты обучения по дисциплине (или модулю)**
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	**Владеть:** методиками анализа результатов работы средств обнаружения вторжений. **Уметь:** формулировать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе. **Знать:** средства и методы хранения и передачи аутентификационной информации.
ПК-11. Способностью участвовать в проведении экспериментально-исследовательских работ при проведении	**Владеть:** навыками настройки межсетевых экранов; методиками анализа сетевого трафика. **Уметь:** применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты.

сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации	**Знать:** механизмы реализации атак в сетях TCP/IP; основные протоколы идентификации и аутентификации абонентов сети; защитные механизмы и средства обеспечения сетевой безопасности; средства и методы предотвращения и обнаружения вторжений.

6. Форма промежуточной аттестации - экзамен

7. Язык преподавания русский**.**