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

Утверждаю:
Руководитель ООП
Н.А. Семыкина
«4» 09 2023 г.

Рабочая программа дисциплины (с аннотацией)

Модели безопасности компьютерных систем

Специальность

10.05.01 Компьютерная безопасность

Специализация

«Математические методы защиты информации»

Для студентов очной формы обучения

СПЕЦИАЛИТЕТ

Для студентов 4 курса ОФО

Составитель:
Семыкина Н. А.

Тверь 2023

I. Аннотация

1. Цель и задачи дисциплины

Целью освоения дисциплины - раскрытие содержания основных понятий и формальных моделей обеспечения безопасности компьютерных систем, а также сформирование теоретико-методологических основ профессиональной деятельности в сфере компьютерной безопасности в контексте всех трех ее составляющих видов — производственно-технологической, организационно-управленческой и экспериментально-исследовательской.

Задачами освоения дисциплины являются:

1) получение базовых знаний и умений, связанных с основными понятиями в сфере компьютерной безопасности;

2) изучение общих принципов анализа и обоснования моделей, методов и механизмов обеспечения компьютерной безопасности;

3) освоение методологии анализа архитектурных (схемно-технических) и программно-алгоритмических решений, применяемых в системах защиты информации современных компьютерных систем.

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».

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

3. Объем дисциплины: 4 зачетные единицы, 144 академических часов, в том числе:

контактная аудиторная работа: лекции – 30 часов, в т.ч. практическая подготовка – 0 часов;

лабораторные занятия – 30 часов, в т.ч. практическая подготовка – 4 часа;

самостоятельная работа: 57 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-8.2** Осуществляет моделирование безопасности компьютерных систем, в том числе моделирование управления доступом и информационными потоками в компьютерных системах
ОПК-11. Способен разрабатывать политики	**ОПК-11.1.** Использует основные формальные модели дискреционного,

безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации	мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков
ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	**ОПК-6.1.** Разрабатывает модели угроз и модели нарушителя компьютерных систем
	ОПК-6.2. Разрабатывает проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации
	ОПК-6.3. Определяет политику контроля доступа работников к информации ограниченного доступа
	ОПК-6.4. Применяет отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы
ОПК-16. Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях	**ОПК-16.1.** Применяет защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях
	ОПК-16.2. Осуществляет меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты

5. Форма промежуточной аттестации и семестр прохождения – экзамен в 8 семестре.

6. Язык преподавания русский**.**