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)

Криптографические протоколы

Специальность

10.05.01 Компьютерная безопасность

Специализация

«Математические методы защиты информации»

Для студентов 5 курса очной формы обучения

Уровень высшего образования

СПЕЦИАЛИТЕТ

Составитель:

ст. преподаватель С.А. Желтов.

Тверь 2023

I. Аннотация

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

Криптографические протоколы.

2. Цель и задачи дисциплины (модуля)

Целью освоения дисциплины (модуля) является:

формирование базы для развития профессиональных компетенций, связанных с готовностью студента к деятельности в области проектирования и построения криптографических протоколов, предназначенных для решения различных профессиональных, исследовательских и прикладных задач.

Задачами освоения дисциплины (модуля) являются:

- получение базовых знаний и умений, связанных с основными понятиями криптографических протоколов;
- получение теоретических знаний о роли и назначении различных криптографических протоколов;
- обучения студентов общим принципам и методам построения криптографических протоколов;
- получение теоретических знаний и практических навыков о основных прикладных задачах, решаемых с помощью криптопротоколов;

3. Место дисциплины (модуля) в структуре ООП

Дисциплина входит в базовую часть профессионального цикла.

Для освоения дисциплины студент должен владеть основными понятиями криптографии, информационной безопасности. Необходимы знания, умения и компетенции, полученные студентами на занятиях по дисциплинам Организационное и правовое обеспечение информационной безопасности, информатика, криптографические методы защиты информации, теоретико-числовые методы в криптографии. Знания и практические навыки, полученные из курса, используются студентами при прохождении производственной и преддипломной практики, а также при разработке курсовых и дипломных работ.

4. Объем дисциплины (или модуля):

___3___ зачетных единиц, __108__ академических часов, **в том числе контактная работа:** лекции _36__ часов, практические занятия _18____ часов, **самостоятельная работа:** ___54__ 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 (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:** навыками освоения большого объема информации и решения задач (в том числе, сложных). **Уметь:** самостоятельно находить информацию по алгоритмам решения задач, в том числе и нестандартных, и проводить их анализ. **Знать:** основы Интернет-технологий, современные проблемы соответствующих разделов криптографии.
Базовый **ПК-3** способностью проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности.	**Владеть:** криптографической терминологией; простейшими подходами к анализу безопасности криптографических протоколов. **Уметь:** использовать симметричные и асимметричные шифрсистемы для построения криптографических протоколов; формулировать свойства безопасности криптографических протоколов; проводить сравнительный анализ криптографических протоколов, решающих сходные задачи. **Знать:** криптографические протоколы, применяемые в компьютерных сетях; формулировать задачу по оцениванию безопасности криптографического протокола применительно к конкретным условиям;

	криптографические стандарты; основные схемы цифровой подписи.

6. Форма промежуточной аттестации:
экзамен.
7. Язык преподавания русский**.**