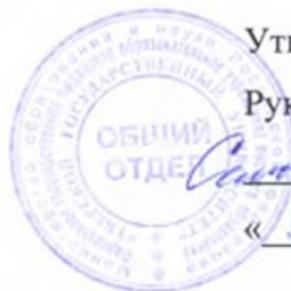


Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Смирнов Сергей Николаевич
Должность: врио ректора
Дата подписания: 16.10.2023 14:57:08
Уникальный программный ключ:
69e375c64f7e975d4e8830e7b4fcc2ad1b35f08


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)

Криптографические методы защиты информации

Специальность

10.05.01 Компьютерная безопасность

Специализация

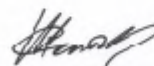
«Математические методы защиты информации»

Для студентов 4 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 методы защиты информации.

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 использования и проектирования и средств криптографической защиты информации, предназначенных для решения различных профессиональных, исследовательских и прикладных задач.

Задачами освоения дисциплины (модуля) являются:

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

3. Место дисциплины (модуля) в структуре ООП

Дисциплина входит в базовую часть профессионального цикла дисциплин.

Для освоения дисциплины студент должен владеть основными понятиями, алгебры, теории вероятности, теории информации, информационной безопасности. Необходимы знания, умения и компетенции, полученные студентами на занятиях по дисциплинам Организационное и правовое обеспечение информационной безопасности, языки программирования, алгебра. 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):

 7 зачетных единиц, 252 академических часов, в том числе **контактная работа:** лекции 66 часов, практические занятия 18 часов, лабораторные работы 48 часов, **самостоятельная работа:** 75 часа, **контроль** 45 часов.

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 (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 определения видов и форм информации, подверженных угрозам, и возможных методов и путей устранения этих угроз. Уметь: пользоваться научно-технической литературой в области криптографии. Знать: основные задачи и понятия криптографии.</p>
<p>Базовый ПСК-2.1. способностью разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации.</p>	<p>Владеть: криптографической терминологией; навыками использования типовых криптографических алгоритмов. Уметь: корректно применять симметричные и асимметричные криптографические алгоритмы; использовать криптографические методы и средства защиты информации в автоматизированных системах. Знать: основные криптографические примитивы и их использование в решении основных задач защиты информации; принципы построения и основные виды симметричных и асимметричных криптографических</p>

	алгоритмов; основные криптографические методы и алгоритмы защиты информации; криптографические стандарты.
Продвинутый ПСК-2.1. способностью разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации.	Владеть: навыками использования ПЭВМ в анализе простейших шифров; навыками математического моделирования в криптографии. Уметь: применять математические методы описания и исследования криптосистем; использовать принципы построения средств криптографической защиты информации. Знать: криптографические алгоритмы и особенности их программной реализации; математические модели шифров; частотные характеристики открытых текстов и их применение к анализу простейших симметричных криптосистем; требования к шифрам и основные характеристики шифров.

6. Форма промежуточной аттестации: зачет, экзамен.

7. Язык преподавания русский.