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)

Методы алгебраической геометрии в криптографии

Специальность

10.05.01 Компьютерная безопасность

Специализация

«Математические методы защиты информации»

Для студентов 5 курса очной формы обучения

Уровень высшего образования

СПЕЦИАЛИТЕТ

Составители:

ст. преподаватель С.А. Желтов.

Тверь 2023

I. Аннотация

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

Методы алгебраической геометрии в криптографии.

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 на эллиптических кривых, предназначенных для решения различных профессиональных, исследовательских и прикладных задач.

Задачами освоения дисциплины (модуля) являются:

- получение базовых знаний и умений, связанных с основными понятиями алгебраической геометрии;
- получение теоретических знаний о роли и назначении различных криптосистем на базе эллиптических кривых;
- обучения студентов общим принципам и методам построения криптографических систем на основе эллиптических кривых;
- получение теоретических знаний и практических навыков о основных методах и алгоритмах дискретного логарифмирования на эллиптических кривых;

3. Место дисциплины (модуля) в структуре ООП

Дисциплина входит в вариативную часть ООП .

Для освоения дисциплины студент должен владеть современными методами и средствами информационных технологий. Необходимы знания, умения и компетенции, полученные студентами на занятиях по дисциплинам алгебра, 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):

2 зачетных единиц, *72* академических часов, **в том числе контактная работа:** лекции 18 часов, практические занятия 18 часов, **самостоятельная работа:** 36 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)**
Базовый уровень ПК-5. Способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	**Владеть:** навыками программирования алгебраических операций в конечных алгебраических структурах, в том числе в группе точек эллиптических и гиперэллиптических кривых, использования систем компьютерной математики для решения профессиональных задач; методами построения быстрых вычислительных алгоритмов алгебры и теории чисел.
	Уметь: проводить предварительное оценивание временной сложности разрабатываемых алгоритмов.
	Знать: принципы применения эллиптических и гиперэллиптических кривых в криптографии.
Базовый уровень ПК-10. Способность оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации.	**Владеть:** необходимыми теоретическими знаниями в областях, связанных с оценкой эффективности реализации систем защиты информации и действующих политик безопасности в компьютерных системах.
	Уметь: оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах.
	Знать: современные программно-аппаратные средства защиты информации, включая средства криптографической защиты информации.

Базовый уровень **ПК-18.** Способность способностью производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации.	**Владеть:** практическими навыками установки, наладки, тестирования и обслуживания современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем. **Уметь:** производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем. **Знать:** современные программно-аппаратные средства обеспечения информационной безопасности компьютерных систем, включая средства криптографической защиты информации.

6. Форма промежуточной аттестации:
зачёт.

7. Язык преподавания русский**.**