


Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф – Аннотация рабочей программы дисциплины		

## АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

### «Методы алгебраической геометрии в криптографии»

**по специальности 10.05.03 «Информационная безопасность автоматизированных систем»  
специализация «Безопасность открытых информационных систем»**

#### 1. Цели и задачи освоения дисциплины

##### Цели освоения дисциплины:

- ознакомление студентов с основными понятиями алгебраической геометрии;
- развитие навыка построения криптографических протоколов на эллиптических кривых.

##### Задачи освоения дисциплины:

- овладение основными идеями и методами построения криптографических систем на основе эллиптических кривых;
- формирование навыков грамотного применения теоретических основ криптографии в постановке практических задач, в решении задач с применением современного теоретического аппарата, в систематизации полученных знаний.

#### 2. Место дисциплины в структуре ОПОП ВО


Дисциплина относится к дисциплинам по выбору (Б1.В.ДВ.2) образовательной программы и читается в 9-м семестре студентам специальности «Информационная безопасность автоматизированных систем» очной формы обучения. Для успешного освоения дисциплины необходимы знания основных фактов из базовых курсов: «Математический анализ», «Алгебра и геометрия», «Дискретная математика», «Информатика», «Криптографические методы защиты информации». Для освоения дисциплины студент должен иметь следующие «входные» знания, умения, навыки и компетенции: основные задачи и понятия криптографии; классификацию шифров по различным признакам; типы основных способов криптоанализа шифров; основные типы электронной подписи.

Дисциплина «Методы алгебраической геометрии в криптографии» является предшествующей для прохождения преддипломной практики и итоговой государственной аттестации.

#### 3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины «Методы алгебраической геометрии в криптографии» направлен на формирование следующих компетенций:

- способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач (ОПК-1);
- способностью корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники (ОПК-2);
- способностью проводить анализ защищенности автоматизированных систем (ПК-3);
- способностью разрабатывать политику информационной безопасности автоматизированной системы (ПК-11);

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф – Аннотация рабочей программы дисциплины		

- способностью участвовать в проектировании средств защиты информации автоматизированной системы (ПК-13).

В результате изучения дисциплины студент должен:

**знать:**

- методы приложения конечных полей в криптографии;
- принципы применения эллиптических кривых в криптографии;
- протоколы эллиптической криптографии;
- протоколы электронной подписи на основе эллиптических кривых;

**уметь:**

- решать задачи на алгебраические многообразия;
- разрабатывать быстрые вычислительные алгоритмы для криптографических приложений;

**владеть:**

- навыками программирования алгебраических операций в конечных алгебраических структурах, в том числе в группе точек эллиптических кривых;
- методами формирования электронных подписей.

#### 4. Общая трудоемкость дисциплины

Общая трудоемкость дисциплины составляет 5 зачетных единиц (180 часов)

#### 5. Образовательные технологии

В ходе освоения дисциплины при проведении аудиторных занятий используются следующие образовательные технологии:

- чтение лекций;
- проведение практических занятий;
- организация самостоятельной образовательной деятельности;
- организация и проведение консультаций;
- проведение экзамена.

При организации самостоятельной работы занятий используются следующие образовательные технологии:

- формирование и усвоение содержания конспекта лекций на базе рекомендованной учебной литературы;
- подготовка к семинарам, их оформление;
- подготовка к лабораторным работам, их оформление.

#### 6. Контроль успеваемости

Программой дисциплины предусмотрены следующие виды текущего контроля: защита лабораторных работ.

Промежуточная аттестация проводится в форме: экзамен.