

Аннотация дисциплины  
Б1.В.ДВ.04.01 Эллиптическая кривая и электронная подпись  
(код и наименование дисциплины)

**Объем трудоемкости:** 2 зач. ед.

**Цель освоения дисциплины.**

Цель освоения дисциплины – рассматривает задачи информатизации и защиты информации. Изучение этой дисциплины является важной составной частью современного математического образования и образования в области компьютерных наук.

**Задачи дисциплины.**

Задачи освоения дисциплины эллиптическая кривая и электронная подпись: получение базовых теоретических и исторических сведений о структуре информатизации, ее развитии, применении этих знаний на практике, перспектив развития математических и компьютерных наук, месте и роли защиты информации в структуре информатизации.

Изучение теоретических основ предмета: автоматизированные системы, функционирующие в условиях существования угроз в информационной сфере и обладающие информационно-технологическими ресурсами, подлежащими защите; информационные технологии, формирующие информационную инфраструктуру в условиях существования угроз в информационной сфере и задействующие информационно-технологические ресурсы, подлежащие защите; технологии обеспечения информационной безопасности автоматизированных систем; системы управления информационной безопасностью автоматизированных систем;

Развитие навыков разработки алгоритмов и практического решения прикладных задач информатизации. Сбор, обработка, анализ и систематизация научно-технической информации, отечественного и зарубежного опыта по проблемам информационной безопасности автоматизированных систем; подготовка научно-технических отчетов, обзоров, публикаций по результатам выполненных исследований.

**Место дисциплины (модуля) в структуре образовательной программы.**

Дисциплина Эллиптическая кривая и электронная подпись относится к части, формируемой участниками образовательных отношений к вариативной части Блока 1 "Дисциплины (модули)" учебного плана Б1.В.ДВ.04.01.

Курс эллиптическая кривая и электронная подпись продолжает, начатое на трех курсах математическое образование и студентов соответствующего направления подготовки. Знания, полученные в этом курсе, могут быть использованы в курсах защита операционных систем и баз данных, криптография, организационно-правовые методы защиты информации и др. Слушатели должны владеть знаниями в рамках программы курсов «Алгебра», «Дискретная математика», «Программирование», «Информатика», «Правоведение».

**Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы**

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих компетенций:

| Код и наименование индикатора* достижения компетенции                                                            | Результаты обучения по дисциплине (знает, умеет, владеет (навыки и/или опыт деятельности))                                                                                                                                                                                                                                  |
|------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ПК-2</b> Способен активно участвовать в исследовании новых математических моделей в естественных науках       |                                                                                                                                                                                                                                                                                                                             |
| ПК-2.1 Умеет использовать математические модели и применять численные методы решения задач в естественных науках | Знать: об основных задачах и понятиях криптографии; о классификации шифров; о методах криптографического синтеза и анализа; о применениях криптографии в решении задач аутентификации, построения систем цифровой подписи;<br>Уметь использовать: типовые шифры замены и перестановки; частотные характеристики языков и их |
| ПК-2.2 Разрабатывает новые математические модели в естественных науках                                           |                                                                                                                                                                                                                                                                                                                             |
| ПК-2.3 Владеет навыками математической обработки результатов                                                     |                                                                                                                                                                                                                                                                                                                             |

| Код и наименование индикатора* достижения компетенции              | Результаты обучения по дисциплине<br>(знает, умеет, владеет<br>(навыки и/или опыт деятельности))                                                                                                                                                                                                     |
|--------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| экспериментальных исследований составленных математических моделей | использование в криптоанализе; требования к шифрам и основные характеристики шифров; принципы построения современных шифрсистем:<br>Владеть: криптографической терминологией; навыками использования основных типов шифров и криптографических алгоритмов; методами криптоанализа простейших шифров: |

**Содержание дисциплины:**

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

| №  | Наименование разделов (тем)                                                                                           | Количество часов |                   |    |    |                      |
|----|-----------------------------------------------------------------------------------------------------------------------|------------------|-------------------|----|----|----------------------|
|    |                                                                                                                       | Всего            | Аудиторная работа |    |    | Внеаудиторная работа |
|    |                                                                                                                       |                  | Л                 | ПЗ | ЛР |                      |
| 1. | Об основных задачах и понятиях криптографии; о классификации шифров; о нормативно-правовых основах защиты информации. | 14               | 2                 |    | 4  | 8                    |
| 2. | Эллиптические кривые над конечными полями и алгоритмы вычисления на них.                                              | 16               | 2                 |    | 4  | 10                   |
| 3. | Табличное и модульное гаммирование.                                                                                   | 14               | 2                 |    | 4  | 8                    |
| 4. | Построение больших простых чисел.                                                                                     | 23,8             | 4                 |    | 8  | 11,8                 |
|    | <b>ИТОГО по разделам дисциплины</b>                                                                                   |                  | 10                |    | 20 | 37,8                 |
|    | Контроль самостоятельной работы (КСР)                                                                                 | 4                |                   |    |    |                      |
|    | Промежуточная аттестация (ИКР)                                                                                        | 0,2              |                   |    |    |                      |
|    | Подготовка к текущему контролю                                                                                        |                  |                   |    |    |                      |
|    | Общая трудоемкость по дисциплине                                                                                      | 72               |                   |    |    |                      |

**Курсовые работы:** не предусмотрены

**Форма проведения аттестации по дисциплине:** зачет

Автор А.В. Рожков, профессор, д.ф.-м.н.