

АННОТАЦИЯ
дисциплины Б1.В.ДВ.14.01 «ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ И ЭЛЕКТРОННАЯ ПОДПИСЬ»

Объем трудоемкости: 2 зачетные единицы (72 ч., из них 50,2 контактных – 48 ч. аудиторной нагрузки: лекционных 24 ч., лабораторные занятия 24 ч., 2 ч. КСР, 0,2 ИКР) 21,8 ч. самостоятельной работы.

Цель дисциплины:

Цель освоения дисциплины – знакомство с задачами и методами защиты информации математическими методами. Изучение этой дисциплины является важной составной частью современного математического образования и образования в области компьютерных наук. Ее значение возрастает в свете ведущейся информационной войны против Российской Федерации.

Задачи дисциплины:

Задачи освоения дисциплины «Эллиптические кривые и электронная подпись»: получение базовых теоретических и исторических сведений о структуре и алгоритмах функционирования криптоалгоритмов. Применение этих знаний на практике, при рассмотрении перспектив развития математических и компьютерных наук, месте и роли защиты информации в структуре информатизации и математических методов построения защищенных информационных систем.

Изучение теоретических основ предмета и получение сведений:

о компьютерной реализации информационных объектов;

связи компьютерной алгебры и численного анализа;

об основных задачах и понятиях криптографии;

об этапах развития криптографии;

о видах информации, подлежащей шифрованию;

о классификации шифров;

о методах криптографического синтеза и анализа;

о применениях криптографии в решении задач аутентификации, построения систем цифровой подписи;

о методах криптозащиты компьютерных систем и сетей.

Место дисциплины в структуре ООП ВО

Дисциплина «Эллиптические кривые и электронная подпись» относится к вариативной части Блока 1 «Дисциплины (модули)» учебного плана и является дисциплиной по выбору студента.

Данная дисциплина, как математическая основа теории защищенных информационных систем, призвана содействовать фундаментализации образования, укреплению правосознания и развитию системного мышления студентов.

Требования к уровню освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	уметь	владеть
1.	ОПК-2	способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением ин-	об основных задачах и понятиях криптографии; о классификации шифров; о методах криптографического	типичные поточные и блочные шифры, системы шифрования с открытыми ключами, криптографи-	навыками использования основных типов шифров и криптографических алгоритмов; методами крипто-

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	уметь	владеть
		формационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	синтеза и анализа;	ческие протоколы;	анализа простейших шифров:
2	ПК-5	способностью использовать методы математического и алгоритмического моделирования при решении теоретических и прикладных задач	о применениях криптографии в решении задач аутентификации, построения систем цифровой подписи	основные математические методы, используемые в анализе типовых криптографических алгоритмов.	навыками математического моделирования в криптографии.

Основные разделы дисциплины:

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1	Об основных задачах и понятиях криптографии; о классификации шифров; о нормативно-правовых основах защиты информации	18	6		6	6
2	Эллиптические кривые над конечными полями и алгоритмы вычисления на них.	18	6		6	6
3	Табличное и модульное гаммирование.	18	6		6	6
4	Построение больших простых чисел.	15,8	6		6	3,8
	<i>Итого по дисциплине:</i>		24		24	21,8

Курсовые работы: не предусмотрены.

Форма проведения аттестации по дисциплине: зачет

Основная литература:

1. Рябко Б.Я, Фионов А.Н. Криптографические методы защиты информации [Электронный ресурс]. – М.: Горячая линия-Телеком, 2012. – URL: <https://e.lanbook.com/book/5193>
2. Глухов М.М., Круглов И.А., Пичкур А.Б., Черемушкин А.В. Введение в теоретико-числовые методы криптографии. [Электронный ресурс]. – СПб.: Лань, 2011. – URL: <https://e.lanbook.com/book/68466>

Автор РПД доктор физ.-мат наук, профессор Рожков А.В.