АННОТАЦИЯ
дисциплины «ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ И ЭЛЕКТРОННАЯ ПОДПИСЬ»

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

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 профессиональному циклу (Б1) к курсам естественно-научного содержания (Б1.В.ДВ.14.01).

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 информационно-коммуни-	об основных задачах и понятиях криптографии; о классификации шифров; о методах криптографического	типовые поточные и блочные шифры, системы шифрования с открытыми ключами, криптографические протоколы;	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**
		кационных технологий и с учетом основных требований информационной безопасности.	синтеза и анализа; о применениях криптографии в решении задач аутентификации, построения систем цифровой подписи	основные математические методы, используемые в анализе типовых криптографических алгоритмов.	анализа простейших шифров: навыками математического моделирования в криптографии.
2	ПК-5	способностью использовать методы математического и алгоритмического моделирования при решении теоретических и прикладных задач			

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.	18	6		6	6
	Итого по дисциплине:	72	24		24	24

Курсовые работы: не предусмотрены.
Форма проведения аттестации по дисциплине: зачет
Основная литература:

1. Аверченков В.И., Рытов М.Ю., Шпичак С.А. Криптографические методы защиты информации: учебное пособие, 2-е изд. [Электронный ресурс]. – М.: ФЛИНТА, 2017 https://e.lanbook.com/book/92914?category_pk=1537.
2. Торстейнсон П., Ганеш Г.А. Криптография и безопасность в технологии .NET. 3-е изд. [Электронный ресурс]. – М.: Лаборатория знаний, 2015. – URL: http://e.lanbook.com/view/book/70724/

Автор РПД Рожков А.В.