

АННОТАЦИЯ
дисциплины «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 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-коммуникационных	об основных задачах и понятиях криптографии; о классификации шифров; о методах криптографического синтеза и анализа;	типовые точные и блочные шифры, системы шифрования с открытыми ключами, криптографические протоколы;	навыками использования основных типов шифров и криптографических алгоритмов; методами криптоанализа простейших шиф-

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	уметь	владеть
		технологий и с учетом основных требований информационной безопасности.	о применениях криптографии в решении задач аутентификации, построения систем цифровой подписи	основные математические методы, используемые в анализе типовых криптографических алгоритмов.	ров: 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.	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. 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/>

Дополнительная литература:

1. Бирюков А.А. Информационная безопасность: защита и нападение, 2-е изд. [Электронный ресурс]. – М.: ДМК Пресс, 2017. – URL: <http://e.lanbook.com/view/book/93278/>
2. Нестеров С.А. Основы информационной безопасности, 3-е изд. [Электронный ресурс]. - СПб.: Лань, 2017. - https://e.lanbook.com/book/90153?category_pk=1537.

3. Чечёта С.И. Введение в дискретную теорию информации и кодирования [Электронный ресурс]. – М.: МЦНМО, 2011. – URL: <http://e.lanbook.com/view/book/9437/>

Нормативно-правовые документы:

1. Федеральный закон. Об электронной подписи от 06.04.2011 № 63-ФЗ (ред. от 23.06.2016 N 220-ФЗ).
2. Федеральный закон. Об информации, информационных технологиях и о защите информации от 27.07.2006 № 149-ФЗ (ред. от 23.04.2018 N 102-ФЗ).
3. Постановление Правительства РФ. Об использовании простой электронной подписи при оказании государственных и муниципальных услуг от 25.01.2013 № 33 (ред. от 25.10.2017 № 1296).
4. ГОСТ Р 34.11–2012. Информационная технология. Криптографическая защита информации. Функция хэширования.
5. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

Интернет-ресурсы:

1. Пакет компьютерной алгебры Sage 8.2. Официальный сайт <http://sagemath.org/>
2. Пакет компьютерной алгебры Gap4r9p1. Официальный сайт <http://www.gap-system.org/>
3. Пакет компьютерной алгебры PARI/GT 2.9. Официальный сайт <http://pari.math.u-bordeaux.fr/>
4. Пакет компьютерной алгебры Maple 2018. <http://www.maplesoft.com>
5. <http://www.pravo.gov.ru> – официальный портал правовой информации
6. <http://www.government.ru> - интернет-портал Правительства РФ
7. <http://graph.document.kremlin.ru> - раздел «Документы» портала Президента России
8. <http://minsvyaz.ru/ru> - сайт Минкомсвязи РФ
9. <http://www.rsoc.ru> - сайт Федеральной службы Роскомнадзор
10. <http://www.scrf.gov.ru> – сайт Совета безопасности РФ
11. <http://base.consultant.ru> – сайт правовой информации «Консультант+»
12. <http://www.fstec.ru> – официальный сайт ФСТЭК России
13. Электронная библиотечная система eLIBRARY.RU (<http://www.elibrary.ru/>)
14. Электронная библиотека <http://gen.lib.rus.ec/>

Автор РПД

Рожков А.В.