

Документ подписан простой электронной подписью
 Информация о владельце:
 ФИО: Петренко Вячеслав Иванович
 Должность: и.о. директора Института цифрового развития

Аннотация дисциплины

Дата подписания: 06.09.2023 12:47:21
 Уникальный программный ключ:
 b47f96eeab5a16e179f94dbf7fb0b10000e/ad4d

Наименование дисциплины	Методы и средства криптографической защиты информации
Краткое содержание	Общие сведения о криптографических методах защиты информации. Классификация шифров. Криптографическая стойкость шифров. Подходы к моделированию криптосистем. Принципы построения и функционирования блочных шифров. Симметричные криптоалгоритмы. Принципы построения и функционирования поточных шифров. Принципы построения криптоалгоритмов с открытым ключом. Современные криптоалгоритмы с открытым ключом. Имитостойкость и помехоустойчивость шифров. Основные методы криптоанализа. Криптоанализ симметричных алгоритмов. Криптоанализ асимметричных алгоритмов. Криптографические хэш-функции. Электронная цифровая подпись. Управление криптографическими ключами. Реализации криптографических алгоритмов: программная, аппаратная, программно-аппаратная. Композиция криптографических методов в систему защиты информации. Криптографические стандарты.
Результаты освоения дисциплины (модуля)	Анализировать и использовать криптографические алгоритмы на практике при решении задач криптографическими методами; применять математические методы при исследовании криптографических алгоритмов; разворачивать инфраструктуру открытых ключей для решения криптографических задач; проводить анализ криптографических протоколов, в том числе с использованием автоматизированных средств. Способен разрабатывать программные и программно-аппаратные средства для систем защиты информации компьютерных систем.
Трудоемкость, з.е.	8
Формы отчетности	Зачет с оценкой; Экзамен
Перечень основной и дополнительной литературы, необходимой для освоения дисциплины	
Основная литература	1. Рябко, Борис Яковлевич. Криптографические методы защиты информации: учеб. пособие для вузов / Б. Я. Рябко, А. Н. Фионов. – М.: Горячая линия – Телеком, 2012. – 229 с.: ил., табл. – Гриф: Рек. УМО. Библиогр.: с. 218-221. – Предм. указ.: с. 222-226. – 500 экз. – ISBN 978-5-9912-0286-2. 2. Бабенко, Л.К. Современные алгоритмы блочного шифрования и методы их анализа / Л.К. Бабенко, Е.А. Ищукова. – М: Гелиос АРВ, 2012. 3. Шанкин, Г.П. Криптография / Г.П. Шанкин, А.В. Бабаш. – М.: Солон-Р, 2012.
Дополнительная литература	1. Гашков, Сергей Борисович. Криптографические методы защиты информации: [учеб. пособие*]. – М.: Академия, 2010. – 299 с. – (Высшее проф. образование). – На обл.: Информационная безопасность. – Предм. указ.: с. 285-286. – Библиогр.: с. 287-294. – ISBN 978-5-7695-4962-5. 2. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. / Б. Шнайер. – М.: Триумф, 2003. 3. Грушо, А.А. Анализ и синтез криптоалгоритмов. Курс лекций / А.А. Грушо, Е.Е. Тимонина, Э.А. Применко. – Йошкар-Ола: МФ МОСУ, 2000.