

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Петренко Вячеслав Иванович
Должность: и.о. директора Института цифрового развития
Дата подписания: 27.09.2022 17:31:15
Уникальный программный ключ:
b47f96eead15c16d179f04b1f7fb0b1000e7ad4d

Аннотация дисциплины

Наименование дисциплины	Методы и средства криптографической защиты информации
Краткое содержание	Основные понятия криптографии. Простейшие шифры подстановки и перестановки. Блочные шифры. Американский стандарт шифрования DES. Практическое применение американского стандарта. Стандарт криптографической защиты AES. Принципы работы алгоритма шифрования AES. Стандарт шифрования данных Магма. Отечественный стандарт шифрования Кузнечик. Синхронные поточные системы шифрования. Самосинхронизирующиеся поточные системы шифрования. Программная реализация шифров. Режимы использования блочных шифров. Режимы шифрования с обратной связью. Надежность шифров. Стойкость шифров. Асимметричные системы шифрования. Практическая реализация асимметричных систем шифрования. Электронная цифровая подпись. Практическая реализация электронных цифровых подписей. Управление ключами. Протоколы распределения ключей. Криптографические схемы разделения секрета. Протоколы аутентификации. Протоколы аутентификации с нулевым разглашением знаний и их применение. Скрытый канал. Принципы построения. Криптографические хеш-функции.
Результаты освоения дисциплины	Обладает способностью использовать принципы построения средств криптографической и технической защиты информации для решения задач профессиональной деятельности.
Трудоемкость, з.е.	5
Формы отчетности	Экзамен
Перечень основной и дополнительной литературы, необходимой для освоения дисциплины	
Основная литература	1. Игнатьев, Е. Б. Основы криптографии. Электронный ресурс / Игнатьев Е. Б. : учебное пособие. - Иваново : ИГЭУ, 2020. - 88 с. - Печатается по решению редакционно-издательского совета ФГБОУВО «Ивановский государственный энергетический университет имени В.И. Ленина», экземпляров неограничено 1. Борисова, С. Н. Криптографические методы защиты информации: классическая криптография. Электронный ресурс / Борисова С. Н. : учебное пособие. - Пенза : ПГУ, 2018. - 186 с. - ISBN 978-5-907102-51-4, экземпляров неограничено
Дополнительная литература	1. Басалова, Г. В. Основы криптографии : учебное пособие / Басалова Г. В. - Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. - 282 с. - Книга находится в базовой версии ЭБС IPRbooks., экземпляров неограничено 2. Кукина, Е. Г. Введение в криптографию : Сборник задач и упражнений / Кукина Е. Г. - Омск : Омский государственный университет им. Ф.М. Достоевского, 2013. - 91 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-7779-1588-7 3. Рябко, Б. Я. Криптографические методы защиты информации : учеб. пособие для вузов / Б. Я. Рябко, А. Н. Фионов. - М. : Горячая линия - Телеком, 2014. - 229 с. : ил., табл. - Гриф: Рек. УМО. - Библиогр.: с. 218-221. - Предм. указ.: с. 222-226. - ISBN 978-5-9912-0286-2, экземпляров 15