

Документ подписан простой электронной подписью
 Информация о владельце:
 ФИО: Петренко Вячеслав Иванович
 Должность: и.о. директора Института цифрового развития
 Дата подписания: 31.05.2023 14:31:13
 Уникальный программный ключ:
 b47f96eead15c64179f044bf7fb0b10000e7ad4d

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.	8 з.е.
Формы отчетности	Зачет с оценкой – 5 семестр Экзамен – 6 семестр
Перечень основной и дополнительной литературы, необходимой для освоения дисциплины	
Основная литература	1.Бутакова, Н. Г. Криптографические методы и средства защиты информации : учебное пособие / Н. Г. Бутакова, Н. В. Федоров. — Санкт-Петербург : Интермедия, 2020. — 380 с. — ISBN 978-5-4383-0210-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/161347 2.Костин, В. Н. Методы и средства защиты компьютерной информации: Криптографические методы для защиты информации : учебное пособие / В. Н. Костин. — Москва : МИСИС, 2018. — 40 с. — ISBN 978-5-90695-334-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/115270
Дополнительная литература	1. Применение искусственных нейронных сетей и системы остаточных классов в криптографии / [авт. кол.: Червяков Н.И., Евдокимов А.А., и др.]. - Москва : ФИЗМАТЛИТ, 2012. - 280 с. : ил. - Прил.: с. 269-279. - Библиогр.: с. 269-279 (191 назв.) и в конце гл. - ISBN 978-5-9221-1386-1.