

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Петренко Вячеслав Иванович
Должность: и.о. директора Института цифрового развития
Дата подписания: 05.06.2023 15:15:51
Уникальный программный ключ:
b47f96eead179f04bf7fb0b10000e7ad4d

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. Басалова, Г. В. Основы криптографии : учебное пособие / Басалова Г. В. - Москва : Интернет-Университет Информационных Технологий (ИНТУ-ИТ), 2016. - 282 с. - Книга находится в базовой версии ЭБС IPRbooks 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
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.