

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Шебзухова Татьяна Александровна

Должность: Директор Пятигорского института (филиал) Северо-Кавказского федерального университета

Дата подписания: 12.09.2023 15:16:42

Уникальный идентификатор:
d74ce93cd40e30275c7ba2f58486412a1c8ef96f

(ЭЛЕКТРОННЫЙ ДОКУМЕНТ)

Аннотация дисциплины

Наименование дисциплины	Безопасность баз данных
Содержание	Основные понятия криптографии. Классические шифры замены. Классические шифры перестановки. Принципы построения современных шифров с симметричным ключом. Современные стандарты симметричного шифрования DES, AES, ГОСТ 28147-89, ГОСТ Р 34.12-2015. Современные алгоритмы шифрования с открытым ключами. Криптосистемы RSA, Эль-Гамала, Рабина. Алгоритмы генерации простых чисел. Проверка чисел на простоту. Сложность криптографических алгоритмов. Аутентификация данных. Электронная цифровая подпись. Алгоритмы ЭЦП: RSA, Эль-Гамала, Шнорра, ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012. Атаки и угрозы схемами ЭЦП. Понятие о структуре и способах построения криптографических протоколов. Классификация криптографических протоколов.
Реализуемые компетенции	способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4);
Результаты освоения дисциплины (модуля)	ПК-4 Знать: реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты; Уметь: участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты; Владеть: способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты.
Трудоемкость, з.е.	4 з.е.
Форма отчетности	Экзамен – 5 семестр
Перечень основной и дополнительной литературы, необходимой для освоения дисциплины	
Основная литература	1. Петров А.А. Компьютерная безопасность. Криптографические методы защиты.- Саратов: Профобразование, 2017.- 446 с.
Дополнительная литература	1. Лапони́на О.Р. Криптографические основы безопасности.- Москва: ИНТУИТ, 2017.- 244 с. 2. Калмыков И.А. Криптографические методы защиты информации.- Ставрополь: СКФУ, 2017.- 109 с.