

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Петренко Вячеслав Иванович
Должность: и.о. директора Института цифрового развития
Дата подписания: 04.09.2023 12:47:21
Уникальный программный ключ:
b47f96eaeab3a18e175f94db7fb0b10000e7ad4d

Аннотация дисциплины

Наименование дисциплины	
Криптографические протоколы	
Краткое содержание	Формальные описания криптографических протоколов. Уязвимости протоколов. Базовые примеры криптографических протоколов. Вероятностные алгоритмы проверки чисел на простоту. Доказательство с нулевым разглашением. Системы шифрования и хэш-функции. Схемы разделения секрета. Дополнительные криптографические примитивы. Общие сведения о протоколах аутентификации. Протоколы односторонней и двусторонней аутентификации. Протоколы электронной подписи (ЭП) на основе протоколов аутентификации. Электронная подпись DSA, ГОСТ, подпись по схеме Эль-Гамала. Стираемая, слепая, совместная и подтверждаемая ЭП. Протоколы голосования и электронной коммерции.
Результаты освоения дисциплины (модуля)	Способен применять знания о криптографических протоколах для организации защищенного хранения информации и защищенного информационного обмена
Трудоемкость, з.е.	4
Формы отчетности	Зачет с оценкой, 7 семестр
Перечень основной и дополнительной литературы, необходимой для освоения дисциплины	
Основная литература	1. Котова, Л.В. Сборник задач по дисциплине «Методы и средства защиты информации» Электронный ресурс: учебное пособие / Л.В. Котова. – М.: Московский педагогический государственный университет, 2015. – 44 с. – Книга находится в базовой версии ЭБС IPRbooks. – ISBN 978-5-4263-0221-1 2. Ищукова, Е. А. Криптографические протоколы и стандарты: учебное пособие / Е.А. Ищукова, Е.А. Лобова; Министерство образования и науки РФ; Южный федеральный университет; Инженерно-технологическая академия. – Таганрог: Издательство Южного федерального университета, 2016. – 80 с.: ил. – http://biblioclub.ru/. – Библиогр. в кн. – ISBN 978-5-9275-2066-4
Дополнительная литература	1. Санников, Лапоница, О.Р. Основы сетевой безопасности. Криптографические алгоритмы и протоколы взаимодействия: учебное пособие / О.Р. Лапоница. – Основы сетевой безопасности. Криптографические алгоритмы и протоколы взаимодействия, 2020-07-28. – М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. – 242 с. – Книга находится в базовой версии ЭБС IPRbooks. – ISBN 5-9556-00020-5 2. Молдовян А.А. Протоколы аутентификации с нулевым разглашением секрета [Электронный ресурс] / Молдовян А.А., Молдовян Д.Н., Левина А.Б. – Электрон. текстовые данные. – Санкт-Петербург: Университет ИТМО, 2016. – 55 с. – Режим доступа: http://www.iprbookshop.ru/68058.html.