Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Гробова Татьяна Анатольевна
Должность: и.о. декана факультета математики и компьютерных наук имени профессора Н.И. Червякова
Дата подписания: 21.05.2025 11:23:37
Уникальный программный ключ:
bd39d4208aa94cf4422feb787c81619d42de79a7

Аннотация дисциплины

| | |
|---|---|
| Наименование дисциплины (модуля) | **Использование алгебраических методов в области защиты информации** |
| Краткое содержание | Введение в криптографию: примеры шифров, модели шифров, применение методов защиты информации. Теоретическая и практическая стойкость криптосистем; обобщенная схема для криптосистем с закрытыми ключами шифрования. Системы симметричного шифрования и их математические модели.<br>Алгебраические основы: поля, подполя, простые поля; характеристика поля; расширения полей; конечные поля; число элементов конечного поля; цикличность мультипликативной группы конечного поля; дискретное логарифмирование в циклической группе; неприводимые полиномы над конечными полями, некоторые их свойства; реализация основных операций конечного поля: сложение, умножение, возведение в степень, обращение. Порождение больших простых чисел: операции с многоразрядными числами; алгоритмы порождения простых чисел; вероятностные тесты на простоту. Генераторы псевдослучайных чисел, проверка качества работы ГПЧ.<br>Системы асимметричного шифрования; односторонние функции; криптографические протоколы; проблемы криптографических протоколов. Последние достижения в криптоанализе.<br>Цифровая подпись: требования к цифровой подписи, стандарты, прямая цифровая подпись, технологии арбитражной цифровой подписи.<br>Эллиптические кривые: общие понятия и канонические уравнения; эллиптическая кривая над конечным полем; порядок эллиптической кривой; элементы эллиптической криптографии. |
| Результаты освоения дисциплины (модуля) | Знает базовые математические модели, используемые в области защиты информации; особенности решения базовых алгебраических задач в области защиты информации.<br>Умеет применять аппарат теории чисел и алгебры для решения профессиональных задач, в том числе с использованием вычислительной техники; использовать методы алгебраического моделирования при решении теоретических и прикладных задач в области защиты информации; находить, анализировать, реализовывать программно и использовать на практике математические алгоритмы защиты информации.<br>Владеет навыками использования алгебраического моделирования при решении теоретических и прикладных задач в области защиты информации; методами компьютерного решения задач с использованием подходов компьютерной алгебры; навыками использования на практике математических алгоритмов защиты информации. |
| Трудоемкость, з.е. | 6 |
| Форма отчетности | зачет, курсовая работа, экзамен |
| **Перечень основной и дополнительной литературы, необходимой для освоения дисциплины (модуля)** | |
| Основная литература | 1. Петров А.А. Компьютерная безопасность. Криптографические методы защиты [Электронный ресурс] / А.А. Петров. − Электрон. текстовые данные. − Саратов: Профобразование, 2017. − 446 с. − ISBN 978-5-4488-0091-7.<br>Режим доступа: http://www.iprbookshop.ru/63800.html<br>2. Романьков В.А. Алгебраическая криптография [Электронный ресурс]: монография / В.А. Романьков. - Электрон. текстовые данные. - Омск: Омский государственный университет им. Ф.М. Достоевского, 2013. - 136 с. - ISBN 978-5-7779-1600-6. Режим |

| | |
|---|---|
| | доступа: http://www.iprbookshop.ru/24868.html |
| Дополнительная литература | 1. Фороузан Б.А. Математика криптографии и теория шифрования / Б.А. Фороузан. - 2-е изд., испр. - Москва: Национальный Открытый Университет «ИНТУИТ», 2016. - 511 с.: ил., схем. - (Основы информационных технологий). - Библиогр. в кн. - ISBN 978-5-9963-0242-0. Режим доступа: http://biblioclub.ru/index.php?page=book&id=428998<br>2. Фомичев В.М. Методы дискретной математики в криптологии / В.М. Фомичев. - Москва: Диалог-МИФИ, 2010. - 436 с.: ил. - Библиогр.: с. 422-428. - ISBN 978-5-86404-234-2. Режим доступа: http://biblioclub.ru/index.php?page=book&id=447668<br>3. Кнауб Л.В. Теоретико-численные методы в криптографии: учебное пособие / Л.В. Кнауб, Е.А. Новиков, Ю.А. Шитов; Министерство образования и науки Российской Федерации, Сибирский Федеральный университет. - Красноярск: Сибирский федеральный университет, 2011. - 160 с. - ISBN 978-5-7638-2113-7. Режим доступа: http://biblioclub.ru/index.php?page=book&id=229582 |