

Приложение к рабочей программе дисциплины
09.04.03 Прикладная информатика (магистратура)
Профиль: « Информационно-аналитическое обеспечение принятия решений»

АННОТАЦИЯ

рабочей программы дисциплины

Прикладная криптография

дисциплина к дисциплинам части учебного плана, формируемой участниками образовательных отношений, .

Очная форма обучения

Общая трудоемкость дисциплины (ЗЕТ / час.)	3/108
Цель изучения дисциплины	изучение основных подходов, методов и алгоритмов современной криптографии.
Содержание дисциплины	Тема 1. Основные понятия криптографии Тема 2. Методы шифрования с закрытым ключом Тема 3. Принципы построения блочных шифров с закрытым ключом Тема 4. Алгоритмы шифрования DES и AES Тема 5. Алгоритм криптографического преобразования данных ГОСТ 28147-89 Тема 6. Криптографические хеш-функции Тема 7. Поточные шифры и генераторы псевдослучайных чисел. Часть 1 Тема 8. Поточные шифры и генераторы псевдослучайных чисел. Часть 2 Тема 9. Введение в криптографию с открытым ключом Тема 10. Основные положения теории чисел, используемые в криптографии с открытым ключом Тема 11. Криптографические алгоритмы с открытым ключом и их использование Тема 12. Электронно-цифровая подпись Тема 13. Совершенно секретные системы Тема 14. Шифрование, помехоустойчивое кодирование и сжатие информации
Формируемые компетенции (коды)	ПК-1 Способность использовать передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС
Коды и наименование индикатора достижения компетенции	ПК-1.1 Демонстрирует знание теории систем и системного анализа, теории управления; инструментов и методов оценки качества, надежности и информационной безопасности ИС; устройства и возможностей современных ИС; нормативно-технических документов, описывающие качество, надежность и информационную безопасность ИС; ПК-1.2 Анализирует исходные данные по качеству, надежности и информационной безопасности ИС; планирует, распределяет и контролирует выполнение работ; разрабатывает регламентные документы в области качества, надежности и информационной безопасности; ПК-1.3 Применяет навыки обеспечения соответствия процесса развертывания ИС у заказчика принятым в организации или проекте стандартам и технологиям; навыки разработки и согласования регламентов по управлению качеством, надежностью и информационной безопасностью ИС; навыки выбора и внедрения инструментов и методов контроля качества
Дисциплины, участвующие в формировании компетенции	Компьютерная безопасность и управление корпоративными информационными системами Поддержка жизненного цикла корпоративных информационных систем Методы и инструментари конкурентной разведки Когнитивная бизнес-аналитика Теория систем и системный анализ (продвинутый уровень) Проектно-технологическая практика Преддипломная практика Выполнение и защита выпускной квалификационной работы
Образовательные технологии	Лекция, Лабораторная работа; Самостоятельная работа студента
Форма промежуточной аттестации	Зачет