

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Б1.В.06 Методы защиты компьютерной информации

по направлению подготовки: 02.03.03 «Математическое обеспечение и администрирование информационных систем»

по профилю «Информационные системы и базы данных»

Квалификация выпускника: БАКАЛАВР

Выпускающая кафедра: ИСУИР

Кафедра-разработчик рабочей программы: «Интеллектуальные системы и управление информационными ресурсами»

1. Цели освоения дисциплины

Целями освоения дисциплины «Методы защиты компьютерной информации» являются:

- а) формирование знаний о методах криптографической защиты компьютерной информации,
- б) обучение способам применения симметричных и асимметричных криптосистем,
- в) раскрытие сущности процессов, происходящих при зашифровании и расшифровании компьютерной информации.

2. Содержание дисциплины

Основные этапы истории развития криптографических методов защиты информации.

Симметричные криптосистемы и их характеристики.

Российский стандарт криптографической защиты компьютерной информации.

Асимметричные криптосистемы и их свойства.

Аутентификация передаваемой информации при помощи электронной цифровой подписи.

Безопасные протоколы передачи компьютерной информации.

3. В результате освоения дисциплины обучающийся должен

1) Знать:

- а) историю развития криптографической защиты информации;
- б) методы построения основных алгоритмов зашифрования и расшифрования компьютерной информации.

2) Уметь:

- а) решать задачи синтеза криптографических алгоритмов защиты компьютерной информации;
- б) применять криптографические методы для построения алгоритмов электронной цифровой подписи.

3) Владеть:

- а) современными методами построения симметричных алгоритмов шифрования компьютерной информации;
- б) основными методами построения асимметричных криптосистем;
- в) методами построения безопасных протоколов передачи компьютерной информации.

Зав. каф. ИСУИР



Кирпичников А.П.