

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Б1.В.ОД.9 Методы защиты информации

по направлению подготовки: 01.03.02 «Прикладная математика и информатика»

по профилю «Прикладная математика и информатика»

Квалификация выпускника: БАКАЛАВР

Выпускающая кафедра: ИСУИР

Кафедра-разработчик рабочей программы: ИСУИР

1. Цели освоения дисциплины

Целями освоения дисциплины «Методы защиты информации» являются:

- а) формирование знаний о методах построения алгоритмов криптографической защиты данных,
- б) обучение способам применения криптосистем с открытым ключом,
- в) раскрытие сущности процессов, происходящих при зашифровании и расшифровании данных.

2. Содержание дисциплины «Методы защиты информации»:

Основные понятия и исторический обзор развития криптографии. Классификация угроз противника. Классификация атак на систему кодирования данных с секретным ключом. Основные типы симметричных криптосистем. Методы перестановки, методы простой и сложной замены и методы гаммирования.

Сети X. Фейстеля и российский стандарт шифрования данных. Имитозащита и контроль целостности потока сообщений.

Односторонние (однаправленные) функции. Основные типы криптосистем с открытым ключом. Открытое распределение ключей.

Понятие электронной цифровой подписи. Решение проблемы аутентификации передаваемой информации при помощи ЭЦП.

3. В результате освоения дисциплины обучающийся должен:

1) Знать

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

2) Уметь

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

3) Владеть

- а) современными методами построения симметричных алгоритмов шифрования данных;
- б) основными методами построения криптосистем с открытым ключом.

Зав.каф. ИСУИР



Кирпичников А.П.