

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Б1.О.26 Защита информации

по направлению подготовки: 09.03.01 «Информатика и вычислительная техника»
по профилю «Автоматизированные системы обработки информации и управления»

Квалификация выпускника: БАКАЛАВР

Выпускающая кафедра: АССОИ

Кафедра-разработчик рабочей программы: ИСУИР

1. Цели освоения дисциплины

Целями освоения дисциплины «Защита 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 шифровании и расшифровывании данных.

2. Содержание дисциплины «Защита 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 (однонаправленные) 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 зашифровывания и расшифровывания 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. АССОИ, профессор

Р.Н. Гайнуллин