АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ
«Защита информации»

Направление подготовки: 09.03.01 «Информатика и вычислительная техника»
Профиль подготовки «Автоматизированные системы обработки информации и управления»
Квалификация выпускника: БАКАЛАВР
Выпускающая кафедра: «Автоматизированных систем сбора и обработки информации»
Кафедра-разработчик рабочей программы: «Интеллектуальных систем и управления информационными ресурсами»

1. Цели освоения дисциплины

Целями освоения дисциплины «Защита информации» являются

а) формирование фундаментальных знаний в области существующих криптографических систем

б) обучение технологии создания криптографических систем

в) обучение способам применения существующих алгоритмов шифрования

г) раскрытие сущности процессов, происходящих в системах

2. Содержание дисциплины

Исторический очерк развития криптографии

Математические основы криптографии. Основные понятия криптографии

Классификация шифров по различным признакам

Шифры перестановки

Шифры замены

Шифры гаммирования

Надежность шифров

Блочные системы шифрования

Поточные системы шифрования

Системы шифрования с открытыми ключами

Идентификация

Криптографические хеш-функции

Цифровые подписи

Протоколы распределения ключей

Управление ключами

3. В результате освоения дисциплины обучающийся должен

1) Знать:

а) основания криптографической защиты информации в организации;

б) основные понятия и требования криптографической защиты информации

2) Уметь:

а) выявлять специфику криптографических угроз информационной безопасности по ряду категорий информации;

б) выделять основания и объекты защиты информации, определять основания и процедуру осуществления криптографической защиты информации;

3) Владеть:

а) навыками определения криптографической стойкости шифрсистем;

б) навыками обоснования выбора криптографических средств для защиты информации.

.

Зав. каф. АССОИ, профессор  Р.Н. Гайнуллин