АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Б1.В.05 Теория криптографического преобразования данных

по направлению подготовки: 01.03.02 «Прикладная информатика и информатика»
по профилю «Прикладная математика и информатика»
Квалификация выпускника: БАКАЛАВР
Выпускающая кафедра: ИСУИР

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

1. Цели освоения дисциплины

Целями освоения дисциплины «Теория криптографического преобразования данных» 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

Основные этапы истории развития криптографических методов защиты данных.
Криптосистемы с секретным ключом.
Российский стандарт криптографической зашиты данных.
Криптосистемы с открытым ключом и их свойства.
Электронная цифровая подпись и защита целостности передачи данных.
Безопасные протоколы передачи данных.

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 зашиты 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;
в) методами построения безопасных протоколов передачи данных.

Зав.каф. ИСУИР Кирпичников А.П.