АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

«МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ»

Направление подготовки (специальность)	10.05.04 Информационно-аналитические системы безопасности
Направленность (профиль) подготовки	Автоматизация информационно-аналитической деятельности
Цель освоения дисциплины	Обеспечение подготовки специалистов в соответствии с требованиями ФГОС ВО и учебного плана по направлению 10.05.04 «Информационно-аналитические системы безопасности», ознакомление студентов с основами теории двоичного кодирования, алгоритмами сжатия, помехоустойчивого кодирования. Дисциплина «**Методы и средства криптографической защиты информации**» рассматривается как теоретическая и прикладная дисциплина, дающая представления об основных математических и алгоритмических подходах, применяемых для хранения, передачи, исправления информации, представленной в двоичных кодах. Дисциплина посвящена изучению основ криптографии и криптографического анализа, применяемых к защите информации в информационных системах. Обучаемые знакомятся с понятием шифров, симметричной и асимметричной криптографии, электронной подписью, хешированием и другими математическими объектами криптографии. Изучаются соответствующие криптографические стандарты, применяемые сегодня в защите информации в России и за рубежом. Подробно рассматриваются: стандарты RSA, DES, GOST1989, и другие. Также уделено внимание перспективным направлениям в криптографии: криптографические протоколы с разглашением и без разглашения, теория алгоритмической сложности и односторонних функций, схемы разделения секрета и некоторые их приложения в задачах идентификации и аутентификации
Общая трудоемкость дисциплины	11 зачетных единиц, 396 часов
Форма промежуточной аттестации	Зачет, экзамен
Краткое содержание дисциплины:	• Введение. Основные задачи криптологии. Криптография и криптографический анализ • Открытый и закрытый тексты, ключ, основные свойства функции шифрования и дешифрования. • Симметричные шифры. Группы подстановок и перестановок. Чистые шифры. Шифры Виженера и Вернама. • Хеш - функции. Хеш - функции, устойчивые в слабом и сильном смысле по отношению к поиску коллизий.. • Блочные Шифры. Стандарты DES, GOST1989. Поточные шифры. Стандарт A5..

	• Криптографические протоколы. Протокол анонимных вычислений. Схемы разделения секрета. Криптография на эллиптических кривых • Сложность математических задач.

Аннотацию рабочей программы составил доцент кафедры ИЗИ к.ф-м.н. Александров А.В.