

**АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ**  
**«МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ»**

<b>Направление подготовки (специальность)</b>	10.03.01 Информационная безопасность
<b>Направленность (профиль) подготовки</b>	Безопасность автоматизированных систем
<b>Цель освоения дисциплины</b>	<p>Обеспечение подготовки бакалавров в соответствии с требованиями ФГОС ВО и учебного плана по направлению 10.03.01 «Информационная безопасность», 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</p>
<b>Общая трудоемкость дисциплины</b>	11 зачетных единиц, 396 часов
<b>Форма промежуточной аттестации</b>	Зачет, экзамен
<b>Краткое содержание дисциплины:</b>	<ul style="list-style-type: none"> <li>• Введение. Основные задачи криптологии. Криптография и криптографический анализ</li> <li>• Открытый и закрытый тексты, ключ, основные свойства функции шифрования и дешифрования.</li> <li>• Симметричные шифры. Группы подстановок и перестановок. Чистые шифры. Шифры Виженера и Вернама.</li> <li>• Хеш - функции. Хеш - функции, устойчивые в слабом и сильном смысле по отношению к поиску коллизий..</li> <li>• Блочные Шифры. Стандарты DES, GOST1989. Поточные шифры. Стандарт А5..</li> </ul>

	<ul style="list-style-type: none"><li>• Криптографические протоколы. Протокол анонимных вычислений. Схемы разделения секрета. Криптография на эллиптических кривых</li><li>• Сложность математических задач.</li></ul>
--	--

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

