Аннотация к рабочей программе дисциплины

«Криптографические методы защиты информации»

Курс учебной дисциплины «Криптографические методы защиты информации» предназначен для обучения студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в базовую часть дисциплин учебного плана Б1.Б.12.05

Трудоемкость дисциплины в зачетных единицах составляет 6 з.е., в академических часах – 216 часов (лекции – 36 часов, практическая работа – 36 часов, лабораторные работы – 36 часов, самостоятельная работа – 54 часа, в том числе 54 часа на подготовку к экзамену). Дисциплина реализуется на 4 курсе в 7 семестре. Форма контроля по дисциплине – экзамен.

Дисциплина «Криптографические методы защиты информации» логически и содержательно связана с такими курсами, как «Математический анализ», «Основы геометрии».

Содержание дисциплины охватывает следующий круг вопросов: основные методы защиты информации, открытые сообщения и их характеристики, основные понятия криптографии, принципы организации шифрованной связи, основные классы шифров и их свойства, надежность шифров, методы математической статистики, теории булевых функций и теории линейных рекуррентных последовательностей в криптографии.

Цель дисциплины - изложить основополагающие принципы защиты информации с помощью криптографических методов и примеров реализации этих методов на практике.

Задачи дисциплины:

- дать основы системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов;
- изучить принципов синтеза и анализа шифров;

- ознакомить с математическими методами, используемых в криптоанализе.

Для успешного изучения дисциплины «Криптографические методы защиты информации» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов (ОПК-2).

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные, профессиональные компетенции (элементы компетенций).

Код и формулировка компетенции	**Этапы формирования компетенции**	
(ОПК-4) способность применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	Знает	методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами
	Умеет	применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами
	Владеет	методикой и методологией научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами
(ОПК-10) способность к самостоятельному построению алгоритма,	Знает	современные языки программирования и программные комплексы
	Умеет	строить алгоритмы

проведению его анализа и реализации в современных программных комплексах	Владеет	навыком самостоятельного построения алгоритма, проведения его анализа и реализацией в современных программных комплексах

Для формирования вышеуказанных компетенций в рамках дисциплины «Криптографические методы защиты информации» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Оценочные средства: собеседование (ОУ-1), коллоквиум (ОУ-2), конспект (ПР-7).