


Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф – Аннотация рабочей программы дисциплины		

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

«Криптографические методы защиты информации»

по специальности 10.05.01 «Компьютерная безопасность»
специализация «Математические методы защиты информации»

1. Цели и задачи освоения дисциплины

Цели освоения дисциплины:

- приобретение общих представлений о криптографических методах и средствах обеспечения информационной безопасности;
- знакомство с важнейшими криптоалгоритмами, принципами их построения.

Задачи освоения дисциплины:

- освоение основных методов выбора алгоритмов для различных применений и оценки их качества;
- дать основы системного подхода к организации защиты информации; принципов синтеза и анализа шифров;
- дать основы математических методов, используемых в криптоанализе.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина относится к факультативным дисциплинам (ФТД.2) образовательной программы и читается в 9-м семестре студентам специальности «Компьютерная безопасность» очной формы обучения.

Для успешного освоения дисциплины необходимы знания основных фактов из базовых курсов: «Алгебра», «Дискретная математика», «Криптографические методы защиты информации», «Информатика».


Для освоения дисциплины студент должен иметь следующие «входные» знания, умения, навыки и компетенции: основные задачи и понятия криптографии; классификацию шифров по различным признакам; типы основных способов криптоанализа шифров; основные типы электронной подписи.

Дисциплина «Криптографические протоколы» является предшествующей для прохождения практики и итоговой государственной аттестации.

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

Процесс изучения дисциплины «Криптографические протоколы» направлен на формирование следующих компетенций.

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
ПК-1 – способностью осуществлять подбор, изучение и обобщение научно-технической информации, нормативных, правовых и методических материалов, отечественного и зарубежного опыта по	Знать: основные виды симметричных и асимметричных криптографических алгоритмов;

Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф – Аннотация рабочей программы дисциплины		

проблемам компьютерной безопасности	
ПК-2 – способностью участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований	Знать: основные виды симметричных и асимметричных криптографических алгоритмов; математические модели шифров; Владеть: криптографической терминологией;
ПК-5 – способностью участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	Знать: основные виды симметричных и асимметричных криптографических алгоритмов; математические модели шифров; Уметь: корректно применять симметричные и асимметричные криптографические алгоритмы; Владеть: криптографической терминологией;
ПК-6 – способностью участвовать в разработке проектной и технической документации	Знать: основные виды симметричных и асимметричных криптографических алгоритмов; математические модели шифров; Уметь: корректно применять симметричные и асимметричные криптографические алгоритмы; Владеть:
ПК-7 – способностью проводить анализ проектных решений по обеспечению защищенности компьютерных систем	Знать: основные виды симметричных и асимметричных криптографических алгоритмов; математические модели шифров; Уметь: корректно применять симметричные и асимметричные криптографические алгоритмы Владеть: криптографической терминологией;

4. Общая трудоемкость дисциплины


Общая трудоемкость дисциплины составляет 2 зачетные единицы (72 часа)

5. Образовательные технологии

В ходе освоения дисциплины при проведении аудиторных занятий используются следующие образовательные технологии:

- чтение лекций;
- проведение практических занятий;
- организация самостоятельной образовательной деятельности;
- организация и проведение консультаций;
- проведение зачетов/экзаменов.

При организации самостоятельной работы занятий используются следующие образовательные технологии:

Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф – Аннотация рабочей программы дисциплины		

- формирование и усвоение содержания конспекта лекций на базе рекомендованной учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);
- подготовка к лабораторным работам, их оформление;
- выполнение курсовой работы.

6. Контроль успеваемости

Программой дисциплины предусмотрены следующие виды текущего контроля: лабораторные работы, проверка решения задач.

Промежуточная аттестация проводится в форме: зачет в 9-м семестре.