

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Б1.В.05 «Основы криптографии»

Цель освоения дисциплины

Цели определены государственным образовательным стандартом высшего образования и соотнесены с общими целями ООП ВО по направлению подготовки «Математическое обеспечение и администрирование информационных систем», в рамках которой преподается дисциплина.

Целью освоения учебной дисциплины «Основы криптографии» является формирование у студентов знаний об основах информационной безопасности и роли криптографической защиты в современном обществе; изучение основных принципов, методов и средств криптографической защиты информации в процессе её обработки, передачи и хранения с использованием компьютерных средств в информационных системах.

Задачи дисциплины

- изучить базовые понятия и математические основы криптографии (теория чисел, модульная арифметика);
- освоить классические симметричные алгоритмы шифрования;
- получить представление об асимметричных криптосистемах, хеш-функциях и электронной подписи;
- выработать навыки практического применения простейших криптографических методов для защиты данных.

Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Основы криптографии» относится к вариативной части Блока 1 «Дисциплины (модули)» учебного плана (индекс Б1.В.05).

Данная дисциплина тесно связана с дисциплинами: «Математический анализ», «Фундаментальные дискретные модели», «Алгебра и теория чисел».

Материал курса может быть использован в дальнейшем при изучении профессиональных дисциплин, связанных с защитой информации и администрированием информационных систем.

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

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих компетенций:

Код и наименование индикатора*	Результаты обучения по дисциплине
УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	
ИД-1.УК-2 Понимает сущность правовых норм, цели и задачи нормативных правовых актов	Знать Основные нормативные правовые акты в сфере защиты информации и криптографии
	Уметь Интерпретировать требования правовых норм применительно к задачам криптографической защиты
	Владеть Пониманием сущности правовых ограничений на использование криптографических средств

Код и наименование индикатора*	Результаты обучения по дисциплине
ИД-2.УК-2 Осуществляет поиск необходимой правовой информации для решения профессиональных задач	Знать Источники правовой информации по вопросам информационной безопасности и криптографии
	Уметь Находить и анализировать нормативные документы, регламентирующие применение криптосредств
	Владеть Навыками работы с правовыми базами данных и поисковыми системами
ИД-3.УК-2 Использует принципы проектной методологии для решения профессиональных задач	Знать Основы проектной методологии применительно к задачам внедрения криптографической защиты
	Уметь Планировать этапы реализации криптографических решений в информационных системах
	Владеть Методами постановки задач и оценки результатов в рамках проектного подхода
ИД-4.УК-2 Выбирает оптимальный способ решения задач, имеющихся ресурсов и ограничений, оценки рисков на основе проектного инструментария	Знать Критерии выбора криптографических алгоритмов с учётом ресурсных и нормативных ограничений
	Уметь Оценивать риски и выбирать наиболее эффективные способы защиты информации
	Владеть Инструментарием для обоснованного принятия решений при выборе криптосредств
ПК-1 Способен применять фундаментальные знания, полученные в области математических и (или) естественных наук, и использовать их в профессиональной деятельности	
ИД-1.ПК-1 Имеет практический опыт научно-исследовательской деятельности в области построения математических моделей, программирования и информационных технологий	Знать математические основы криптографии (теория чисел, модульная арифметика, конечные поля)
	Уметь Строить простейшие математические модели криптографических алгоритмов
	Владеть Навыками программной реализации базовых криптографических методов
ИД-2.ПК-1 Умеет находить, формулировать и решать стандартные задачи в конкретной проблемной области	Знать Типовые задачи криптографической защиты информации (шифрование, аутентификация, контроль целостности)
	Уметь Формулировать задачи защиты данных и выбирать подходящие криптографические методы для их решения
	Владеть практическими навыками решения стандартных задач с использованием готовых криптобиблиотек

Структура дисциплины

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы (темы) дисциплины, изучаемые в 8 семестре, форма обучения очная.

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1.	Введение в криптографию. Основные понятия и история развития. Криптостойкость	10	4		4	2
2.	Математические основы криптографии: теория чисел, модульная арифметика, конечные поля, многочлены над полем	12	6		4	2
3.	Классические шифры: шифры замены, перестановки, гаммирования	12	6		4	2
4.	Симметричная криптография. Системы шифрования (DES, AES)	14	6		6	2
5.	Асимметричная криптография. Алгоритм RSA. Хеш-функции. Электронная цифровая подпись	12,8	4		5	3,8
6.	Протоколы распределения ключей (Диффи-Хеллман). Идентификация и аутентификация. Правовые аспекты криптографии в РФ	9	2		5	2
ИТОГО по разделам дисциплины		69,8	28		28	13,8
Контроль самостоятельной работы (КСР)		2				
Промежуточная аттестация (ИКР)		0,2				
Общая трудоемкость по дисциплине		72				

Курсовые работы: не предусмотрены

Форма проведения аттестации по дисциплине: зачет

Автор: Осипян В.О. – д. ф.-м. н., профессор КАДИИ