АННОТАЦИЯ

дисциплины «Б1.О.07 – Криптография и сетевая безопасность»

Направление подготовки/специальности 01.04.02 Прикладная математика и информатика.

Направленность: Технологии программирования и разработки информационно-коммуникационных систем

Объем трудоемкости: 5 зачетных единиц

Цель дисциплины:

Цели изучения дисциплины «Криптография и сетевая безопасность» определены федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению 01.04.02 Прикладная математика и информатика направленность (профиль) " Технологии программирования и разработки информационно-коммуникационных систем" в рамках которой преподается дисциплина.

Задачи дисциплины:

Основной задачей освоения дисциплины является овладение студентами знаниями и практическими навыками, необходимыми для проектирования и разработки безопасных информационных систем и криптографических систем защиты информации.

Место дисциплины в структуре ООП ВО

Дисциплина «Криптография и сетевая безопасность» относится к «Обязательная часть» Блока 1 «Дисциплины (модули)» учебного плана. Для изучения дисциплины необходимо знание материала университетского курса по алгебре, дискретной математике и криптографии. Знания, получаемые при изучении дисциплины «Криптография и сетевая безопасность», используются при изучении таких дисциплин учебного плана магистра как «Интеллектуальные информационные системы и технологии», «Спецсеминар», «Методы извлечения информации из сетевых источников», «Вероятностные модели компьютерных сетей», научно-исследовательская работа, технологическая(проектно-технологическая) практика.

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

Код и наименование индикатора*	Результаты обучения по дисциплине *(знает, умеет, владеет (навыки и/или опыт деятельности))*
ОПК-1. Способен находить, формулировать и решать актуальные проблемы прикладной математики, фундаментальной информатики и информационных технологий.	
ОПК-1.1. Обладает фундаментальными знаниями в области математических и естественных наук, теории коммуникаций.	Знает основы построения математических моделей систем защищенной передачи информации.
ОПК-1.2. Умеет осуществлять первичный сбор и анализ материала, интерпретировать различные математические объекты.	Умеет осуществлять первичный сбор и анализ материала, интерпретировать различные математические объекты как основы построения криптографических алгоритмов.
ОПК-1.3. Имеет практический опыт работы с решением математических задач и применяет его в профессиональной деятельности.	Имеет практический опыт работы с решением задач теории чисел, статистического анализа, дискретной математики.
ОПК-2. Способен применять компьютерные/суперкомпьютерные методы, современное программное обеспечение (в том числе отечественного производства) для решения задач профессиональной деятельности.	
ОПК-2.1. Знает основные положения и концепции в области программирования, архитектуру языков программирования, теории коммуникации, знает основную терминологию, знаком с перечнем ПО, включенного в Единый Реестр Российских программ.	Знает основные положения и концепции в области программирования, архитектуру языков программирования, теории коммуникации, знает основную терминологию, знаком с перечнем ПО по защите информации, включенного в Единый Реестр Российских программ.
ОПК-2.2. Умеет анализировать типовые языки программирования, составлять программы.	Умеет анализировать типовые языки программирования и выбирать наилучший для реализации конкретного алгоритмы защиты информации, составлять программы безопасной передачи и хранения данных.
ОПК-2.3. Имеет практический опыт решения задач анализа, интеграции различных типов программного обеспечения, анализа типов	Имеет практический опыт решения задач анализа, интеграции программного обеспечения сетевой безопасности в действующие информационные и программные системы, анализа типов

Код и наименование индикатора*	Результаты обучения по дисциплине *(знает, умеет, владеет (навыки и/или опыт деятельности))*
коммуникации.	коммуникации.
ОПК-3. Способен проводить анализ математических моделей, создавать инновационные методы решения прикладных задач профессиональной деятельности в области информатики и математического моделирования.	
ОПК-3.1. Знает методы теории алгоритмов, методы системного и прикладного программирования, основные положения и концепции в области математических, информационных и имитационных моделей.	Знает методы теории алгоритмов, методы системного и прикладного программирования, основные положения и концепции в области математических, информационных и имитационных моделей систем безопасности данных
ОПК-3.2. Умеет соотносить знания в области программирования, интерпретацию прочитанного, определять и создавать информационные ресурсы глобальных сетей, образовательного контента, средств тестирования систем.	Умеет соотносить знания в области программирования, интерпретацию прочитанного, определять и создавать информационные ресурсы глобальных сетей, образовательного контента, средств тестирования систем с учетом требований к безопасности информации
ОПК-3.3. Имеет практический опыт применения разработки программного обеспечения и тестирования программных продуктов.	Имеет практический опыт применения разработки программного обеспечения, реализующего или использующего современные криптографические протоколы

Содержание и структура дисциплины (модуля)

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

№ раздела	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1.	Базовые понятия и история развития информационной безопасности.	22	2		2	18
2.	Конечные поля. Многочлены над конечным полем. Последовательности над конечным полем.	22	2		2	18
3.	Шифры замены. Шифры перестановки. Шифры гаммирования.	22	2		2	18
4.	Блочные системы шифрования.	26	4		4	18
5.	Поточные системы шифрования.	26	4		4	18
6.	Идентификация. Цифровые подписи.	26	4		4	18
	ИТОГО по разделам дисциплины	144	18		18	108
	Контроль самостоятельной работы (КСР)					
	Промежуточная аттестация (ИКР)	0,3				
	Подготовка к текущему контролю	35,7				
	Общая трудоемкость по дисциплине	180				

Курсовые работы: не предусмотрены

Форма проведения аттестации по дисциплине: (экзамен)

Основная литература

1. Прохорова, О.В. Информационная безопасность и защита информации : учебник / О.В. Прохорова ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет». - Самара : Самарский государственный архитектурно-строительный университет, 2014. - http://biblioclub.ru/index.php?page=book&id=438331.

2. Лапонина, О.Р. Криптографические основы безопасности / О.Р. Лапонина. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016.

3. Петренко, В.И. Теоретические основы защиты информации : учебное пособие / В.И. Петренко ; Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет». - Ставрополь : СКФУ, 2015. – https://biblioclub.ru/index.php?page=book_red&id=458204&sr=1

4. Фороузан, Б.А. Математика криптографии и теория шифрования / Б.А. Фороузан. - 2-е изд., испр. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - https://biblioclub.ru/index.php?page=book_red&id=428998&sr=1

Автор: В.О. Осипян, проф., доктор физ.-мат. наук