Аннотация дисциплины

Б1.О.09 «ЗАЩИТА ИНФОРМАЦИИ»

Направление подготовки магистров
01.04.02 «Прикладная математика и информатика»
Курс *1* Семестр *2* Трудоемкость *4* з.е.

Цель дисциплины: овладение основными методами защиты информации и их применения при решении задач информационной безопасности, умение самостоятельно расширять знания в области защиты информации.

Задачи дисциплины:

- изучение основных понятий и методов решения типовых задач защиты информации;
- овладение практическими навыками в реализации алгоритмов криптографии;
- обучение основам проведения криптоанализа.

Место дисциплины в структуре ООП ВО:

Дисциплина «Защита информации» относится к обязательной части (Б1.О) учебного плана.

Для изучения данной учебной дисциплины (модуля) студент должен владеть обязательным минимумом содержания математической части ООП для данного направления:

знать/понимать

- основные понятия и методы математического анализа, аналитической геометрии, линейной алгебры, принципы алгоритмизации и программирования;
- основы информационной безопасности;

уметь

- применять математические методы для решения практических задач;
- составлять алгоритмы и компьютерные программы;

владеть

- методами решения алгебраических уравнений, аналитической геометрии, теории вероятностей;
- инструментальными средствами программирования.

Вышеуказанные знания, умения и навыки формируются предшествующими дисциплинами:

- Векторная алгебра.
- Математический анализ.
- Основы информационной безопасности.
- Основы программирования.

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

Изучение данной учебной дисциплины направлено на формирование у обучающихся общепрофессиональных компетенций (ОПК):

№ п.п.	Код и наименование компетенции	Индикаторы достижения компетенции		
		знает	**умеет**	**владеет**
1.	ОПК-4 Способен комбинировать и адаптировать существующие ин-	- основные понятия о погрешности и приближенных вычислениях;	обоснованно выбрать вычислительный метод, разработать алгоритм реше-	инструментарием разработки программной реализации криптографи-

№ п.п.	Код и наименование компетенции	Индикаторы достижения компетенции		
		знает	**умеет**	**владеет**
	формационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности	- основные требования, предъявляемые к вычислительным схемам: корректность, устойчивость, сходимость;	ния поставленной задачи в рамках теоретического и экспериментального исследования;	ческих алгоритмов
2.	ПК-3 Способен эффективно применять алгоритмические и программные решения в области информационно-коммуникационных технологий, а также участвовать в их проектировании и разработке	- криптографические методы защиты информации; - протоколы безопасности	составить и отладить программу на алгоритмическом языке (Паскаль / C++/ Phyton/ Julia) для решения сложных задач (криптографических)	вычислительными методами решения задач линейной алгебры, теории чисел, методами дискретной математики

Содержание и структура дисциплины

№ раздела	Наименование разделов, *тем*	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1.	Системы безопасности с особыми условиями: системы с открытым ключом, разделённый секрет, протокол с нулевым разглашением	46	6	-	6	34
2.	Методы атаки на системы защиты информации и способы противодействия им	42	4	-	4	34
	ИТОГО по разделам дисциплины:	**88**	**10**	-	**10**	**68**
	Промежуточная аттестация (ИКР)	0,3				
	Подготовка к текущему контролю (ПТК)	12				
	Реферат (Р)	8				
	Подготовка к текущему контролю	35,7				
	Общая трудоемкость по дисциплине	**144**				

Сокращения: Л – лекции, ПЗ – практические занятия, ЛР – лабораторные работы, СРС – самостоятельная работа студентов.

Курсовые проекты или работы: *не предусмотрены*

Интерактивные образовательные технологии, используемые в аудиторных занятиях:

Лекционные материалы реализуются с помощью электронных презентаций. При реализации учебной работы по дисциплине «Защита информации» используются следующие образовательные технологии: интерактивная подача материала с мультимедийной системой; разбор конкретных задач по защите информации.

Вид аттестации: *экзамен.*

Основная литература

1. Фомичев, В. М. Криптография — наука о тайнописи: учебное пособие / В. М. Фомичев. - Москва: Прометей, 2020. - 66 с. - ISBN 978-5-00172-040-9. - Текст: электронный. - Режим доступа: https://znanium.com/read?id=389799
2. Бабаш, А. В. Криптографические методы защиты информации.Т.1:Уч.-метод.пос./Бабаш А. В., 2-е изд. - Москва: ИЦ РИОР, НИЦ ИНФРА-М, 2018. - 413 с.: - (Высшее образование: Бакалавриат). - ISBN 978-5-369-01267-3. - Текст: электронный. - Режим доступа: https://znanium.com/read?id=334834
3. Нестеров С. А. Основы информационной безопасности: Учебное пособие. – 3е изд., стер. – СПб.: Издательство «Лань», 2017. – 324 с. – (Учебники для вузов. Специальная литература).ISBN 978-5-8114-2290-6.

5.2 Дополнительная литература

4. Криптографическая защита информации: учебное пособие / С.О. Крамаров, О.Ю. Митясова, С.В. Соколов [и др.]; под ред. С.О. Крамарова. — Москва: РИОР: ИНФРА-М, 2023. — 321 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1716-6. - ISBN 978-5-369-01716-6. - Текст: электронный. - Режим доступа: https://znanium.com/read?id=416723

Автор: доцент кафедры прикладной математики, к.т.н., Савин В.Н.