Аннотация дисциплины

Б1.В.04 «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление подготовки бакалавров
01.03.02 «Прикладная математика и информатика»
Курс *4* Семестр *7* Трудоемкость *3* з.е.

1.1 Цель дисциплины: развитие логического мышления, овладение основными методами обеспечения информационной безопасности, в том числе криптографических, умение самостоятельно расширять знания в области обеспечения информационной безопасности.

1.2 Задачи дисциплины

- изучение основных понятий и методов решения типовых задач информационной безопасности;
- овладение практическими навыками в реализации информационной безопасности.

1.3 Место дисциплины в структуре образовательной программы

Дисциплина «Основы информационной безопасности» относится к части, формируемой участниками образовательных отношений (Б1.В) 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;

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:

- Алгебра и аналитическая геометрия.
- Математический анализ.
- Основы программирования.

Перечень последующих учебных дисциплин, для которых необходимы знания, умения и навыки, формируемые данной учебной дисциплиной:

- Новые информационные технологии в экономике.

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):

№		Индикаторы достижения компетенции

п.п.	Код и наименование компетенции	**знает**	**умеет**	**владеет**
1.	УК-2 Способен определять круг задач в рамках по-	- основные требования, предъявляемые к криптографиче-	обоснованно выбрать криптографический метод, раз-	методами анализа существующих алгоритмов шиф-
№ п.п.	Код и наименование компетенции	Индикаторы достижения компетенции		
		знает	**умеет**	**владеет**
	ставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	ских системам: конфиденциальность, целостность, доступность	работать алгоритм решения поставленной задачи в рамках теоретического и экспериментального исследования;	рования
2.	ОПК-1 Способен применять фундаментальные знания, полученные в области математических и (или) естественных наук, и использовать их в профессиональной деятельности	- вычислительные методы в алгебре; - методы приближенного вычисления сеточных функций;	понимать принципы работы современных информационных технологий и программных средств, в которых применяются численные методы	вычислительными методами решения задач линейной алгебры, оптимизационных задач для функции одной и нескольких переменных, методами дискретной математики и функционального анализа
3.	ПК-3 Способен ориентироваться в современных алгоритмах компьютерной математики; обладать способностями к эффективному применению и реализации математически	- криптографические методы защиты информации	составить и отладить программу на алгоритмическом языке (Паскаль / C++/ Phyton/ Julia) для решения несложных крипто-графических задач	инструментарием разработки программной реализации вычислительных алгоритмов

	сложных алгоритмов			

Содержание и структура дисциплины

№ раздела	Наименование разделов, *тем*	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1.	Введение в основы информационной безопасности	6	2	-	2	2
	1. Исторический обзор применения средств сокрытия информации. История криптографии.	*6*	*2*	-	*2*	*2*
2.	Основные классы шифров и их свойства	16	6	-	6	4
	1. Шифры перестановки.	*6*	*2*	-	*2*	*2*
	2. Блочные шифры замены	*10*	*4*	-	*4*	*2*
3.	Надёжность шифров	12	4	-	4	4
	Основы теории К. Шеннона. Криптографическая стойкость шифров. Теоретически стойкие шифры. Практически стойкие шифры.	*12*	*4*	-	*4*	*4*
4.	Методы синтеза и анализа симметричных шифрсистем	20	8	-	8	4
	1. Управление открытыми ключами.	*10*	*4*	-	*4*	*2*
	2 Методы анализа криптографических алгоритмов.	*10*	*4*	-	*4*	*2*
5.	Методы синтеза и анализа асимметричных криптосистем	20	8	-	8	4
	1 Системы шифрования с открытым ключом.	*10*	*4*	-	*4*	*2*
	2 Алгоритмы идентификации на основе асимметричных криптосистем.	*10*	*4*	-	*4*	*2*
6.	Хеш-функции и их криптографические приложения	14	6	-	6	2
	Хеш-функции и аутентификация сообщений. Общие сведения о хеш-функциях.	*14*	*6*	-	*6*	*2*

	ИТОГО по разделам дисциплины:	**88**	**34**	**0**	**34**	**20**
	Контроль самостоятельной работы (КСР)	4				
	Промежуточная аттестация (ИКР)	0,2				
	Подготовка к текущему контролю	15,8				
	Общая трудоемкость по дисциплине	**108**				

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 «Основы информационной безопасности» используются следующие образовательные технологии: интерактивная подача материала с мультимедийной системой; разбор конкретных исследовательских задач. **Вид аттестации**: зачет.

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

Дополнительная литература

3. 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.