

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 следующих компетенций:

Код и наименование индикатора*	Результаты обучения по дисциплине
УК-3 Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде	
Знать ИУК-3.1 (Зн.1) Проблемы подбора эффективной команды ИУК-3.3 (Зн.3) Основы стратегического управления человеческими ресурсами,	Уметь ИУК-3.13 (06.001 D/03.06 У.3) Осуществлять осуществлять социальное взаимодействие, коммуникации с заинтересованными сторонами Владеть

Код и наименование индикатора*	Результаты обучения по дисциплине
нормативные правовые акты, касающиеся организации и осуществления профессиональной деятельности ИУК-3.4 (Зн.4) Модели организационного поведения, факторы формирования организационных отношений ИУК-3.5 (Зн.5) Стратегии и принципы командной работы, основные характеристики организационного климата и взаимодействия людей в организации	ИУК-3.15 (В.1) Организацией и управлением командным взаимодействием в решении поставленных целей ИУК-3.18 (В.4) Составлением деловых писем с целью организации и сопровождения командной работы
ПК-4 Способен активно участвовать в разработке системного и прикладного программного обеспечения	
Знать ИПК-4.1 (06.001 D/03.06 Зн.1) Принципы построения архитектуры системного и прикладного программного обеспечения и виды архитектуры системного и прикладного программного обеспечения ИПК-4.5 (06.015 В/16.5 Зн.3) Архитектура, устройство и функционирование вычислительных систем используемых в разработке системного и прикладного программного обеспечения ИПК-4.7 (06.016 А/06.6 Зн.1) Возможности ИС, предметная область системное и прикладное программное обеспечение ИПК-4.8 (06.016 А/30.6 Зн.1) Управление рисками проекта при разработке системного и прикладного программного обеспечения ИПК-4.9 (06.016 А/30.6 Зн.2) Возможности ИС, методы разработки прикладного программного обеспечения	Уметь ИПК-4.10 (06.001 D/03.06 У.1) Использовать существующие типовые решения и шаблоны проектирования системного и прикладного программного обеспечения ИПК-4.12 (06.016 А/30.6 У.2) Планировать работы в проектах разработки системного и прикладного программного обеспечения Владеть ИПК-4.17 (06.016 А/30.6 Тд.1) Качественный анализ рисков при разработке системного и прикладного программного обеспечения
ПК-8 Способен планировать необходимые ресурсы и этапы выполнения работ в области информационно-коммуникационных технологий, составлять соответствующие технические описания и инструкции	
Знать ИПК-8.2 (06.016 А/30.6 Зн.1) Управление рисками проекта, способы планирования необходимых ресурсов и этапы выполнения работ в области информационно-коммуникационных технологий, составлять соответствующие технические описания и инструкции ИПК-8.3 (40.001 А/02.5 Зн.3) Методы, этапы и средства планирования и организации исследований и разработок ИПК-8.4 (06.015 В/16.5 У.1) Устанавливать программное обеспечение	Уметь ИПК-8.5 (06.016 А/06.6 У.1) Разрабатывать документы, составлять соответствующие технические описания и инструкции ИПК-8.6 (06.016 А/30.6 У.2) Планировать работы в проектах, необходимые ресурсы и этапы выполнения работ в области информационно-коммуникационных технологий ИПК-8.7 (40.001 А/02.5 У.2) Оформлять результаты научно-исследовательских и опытно-конструкторских работ, составлять соответствующие технические описания и инструкции Владеть ИПК-8.9 (06.016 А/06.6 Тд.1) Подготовка договоров в проектах в соответствии с типовой формой, составление соответствующих технических описаний и инструкций ИПК-8.12 (40.001 А/02.5 Др.2 Тд.) Деятельность, направленная на решение задач аналитического характера, предполагающих выбор и многообразие актуальных способов решения задач, планирование необходимых ресурсов и этапов выполнения работ в области информационно-коммуникационных технологий, составлять соответствующие технические описания и инструкции

Результаты обучения по дисциплине достигаются в рамках осуществления всех видов контактной и самостоятельной работы обучающихся в соответствии с утвержденным учебным планом.

Содержание и структура дисциплины

№ раз-дела	Наименование разделов, тем	Количество часов				
		Все го	Аудиторная работа			Внеауди-торная ра-бота
			Л	ПЗ	ЛР	
1.	Введение в основы информационной безопасности	6	2	-	2	2
	<i>1. Исторический обзор применения средств сокрытия информации. История криптографии.</i>	6	2	-	2	2
2.	Основные классы шифров и их свойства	16	6	-	6	4
	<i>1. Шифры перестановки.</i>	6	2	-	2	2
	<i>2. Блочные шифры замены</i>	10	4	-	4	2
3.	Надёжность шифров	12	4	-	4	4
	<i>Основы теории К. Шеннона. Криптографическая стойкость шифров. Теоретически стойкие шифры. Практически стойкие шифры.</i>	12	4	-	4	4
4.	Методы синтеза и анализа симметричных шифр-систем	20	8	-	8	4
	<i>1. Управление открытыми ключами.</i>	10	4	-	4	2
	<i>2 Методы анализа криптографических алгоритмов.</i>	10	4	-	4	2
5.	Методы синтеза и анализа асимметричных крип-тосистем	20	8	-	8	4
	<i>1 Системы шифрования с открытым ключом.</i>	10	4	-	4	2
	<i>2 Алгоритмы идентификации на основе асим-метричных криптосистем.</i>	10	4	-	4	2
6.	Хеш-функции и их криптографические приложе-ния	14	6	-	6	2
	<i>Хеш-функции и аутентификация сообщений. Об-щие сведения о хеш-функциях.</i>	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 заня-тиях: Лекционные материалы реализуются с помощью электронных презентаций. При ре-ализации учебной работы по дисциплине «Основы информационной безопасности» ис-пользуются следующие образовательные технологии: интерактивная подача материала с мультимедийной системой; разбор конкретных исследовательских задач.

Вид аттестации: зачет.

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