Аннотация к рабочей программы дисциплины
«ФТД.03 ЦИФРОВАЯ БЕЗОПАСНОСТЬ »

Объем трудоемкости: 2 зачетных единиц

Цель дисциплины: Цель освоения дисциплины – решение задач информатизации и защиты информации. Изучение этой дисциплины является важной составной частью современного математического образования и образования в области компьютерных наук.

Задачи дисциплины:

Задачи освоения дисциплины «Цифровая безопасность»: Изучение основных концепций, терминологии и принципов цифровой безопасности, приобретение практических навыков в области защиты сетевых инфраструктур и управления доступом, разработка и анализ политик безопасности и систем управления информационной безопасностью.

Место дисциплины в структуре образовательной программы

Дисциплина «Цифровая безопасность» является факультативной дисциплиной. В соответствии с рабочим учебным планом дисциплина изучается на 3 курсе по очной форме. Вид промежуточной аттестации: зачет.

Курс «Цифровая безопасность» продолжает начатое на двух курсах математическое образование и студентов соответствующего направления подготовки.. Слушатели должны владеть знаниями в рамках программы курсов «Алгебра», «Дискретная математика и математическая логика», «Технологии программирования и работы на ЭВМ»,.

Требования к уровню освоения дисциплины

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

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине (знает, умеет, владеет (навыки и/или опыт деятельности))
ОПК-5. Способен разрабатывать алгоритмы и компьютерные программы, пригодные для практического применения	
ОПК-5.1 Алгоритмизирует задачи на основе существующих методов и стандартных решений при разработке компьютерных программ ОПК-5.2 Реализует алгоритмы с использованием современных средств разработки прикладного программного обеспечения	Знать: о целях, задачах, принципах и основных направлениях обеспечения информационной безопасности государства; о методологии создания систем защиты информации; Уметь: выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации; применять полученные знания при выполнении курсовых проектов и выпускных квалификационных работ, а также в ходе научных исследований; Владеть: анализом информационной инфраструктуры государства; формальной постановкой и решением задачи обеспечения информационной безопасности компьютерных систем.

Содержание дисциплины:

Разделы дисциплины, изучаемые в **шестом** семестре

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1.	Аппаратная часть компьютерных и информационных сетей. Протоколы интернета, выбор операционной системы. Устройство компьютера, основное программное обеспечение.	16	4		4	8

2.	Техническое обслуживание компьютера. Аппаратные неполадки. Работа с BIOS. Ошибки подключении внешних устройств, звук, монитор, принтер, сканер, фото, видео, ТВ, телефон-смартфон. Блоки питания, вентиляторы, источники питания. Дефрагментация диска и др.	16	4		4	8
3.	Программная защита компьютера. Восстановление потерянных данных. Обслуживание HDD и SSD. Антивирусы, наблюдение за периметром сети – вайерволы, защита от спама. Восстановление работоспособности сети. Анализ защищенности сети средствами пакета Kali Linux.	16	4		6	8
4.	Защита личной информации в интернете, смартфоне и компьютере. Проект Tor и VPN-анонимайзер. Шифрование файлов. Электронная подпись. Скачивание файлов. Облачные сервисы. Пять статьи УК РФ за компьютерные нарушения. Гл. 13 Административного кодекса РФ наказания за нарушения в области связи. Основные законы в области защиты информации.	5,8	4		4	9,8
	ИТОГО по разделам дисциплины	67,8	16		18	33,8
	Контроль самостоятельной работы (КСР)	4				
	Промежуточная аттестация (ИКР)	0,2				
	Подготовка к текущему контролю					
	Общая трудоемкость по дисциплине	72				

Курсовые работы: не предусмотрена
Форма проведения аттестации по дисциплине: зачет

Автор: доктор. физ.-мат. наук, профессор Рожков А. В.