Аннотация рабочей программы дисциплины
ФТД.В.01 Методы криптографии и защиты информации

Курс 4 Семестр 7 Количество 1 з.е.

Цель дисциплины - подготовка обучающихся посредством обеспечения этапов формирования компетенций, предусмотренных ФГОС, в части представленных ниже знаний, умений и навыков.

Задачи дисциплины:

1) изучение понятийного аппарата дисциплины, основных теоретических положений и методов;

2) формирование умений и привитие навыков применения теоретических знаний для решения практических и прикладных задач;

Место дисциплины в структуре ООП ВО

Дисциплина «Методы криптографии и защиты информации» относится к вариативной части факультативного блока учебного плана.

Дисциплина «Методы криптографии и защиты информации» учитывает накопленный опыт практической работы магистрантов в образовательных учреждениях, расширяет рамки представлений о сущности образования через освоение подходов к современной классификации наук и месте образования в этой классификации, раскрывает философские проблемы становления человека, методы получения современного научного знания в области образования, а также образовательные инновации, проекты, критерии оценки их эффективности. Изучение дисциплины является основой для последующего изучения дисциплин профессионально-педагогического цикла. Дисциплина базируется на знаниях, полученных при изучении дисциплин «Основы теории кодирования», «Управление данными», «Теория информационных процессов и систем».

Результаты обучения (знания, умения, опыт, компетенции):

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
1.	ПК-25	способность использовать математические методы обработки, анализа и синтеза результатов профессиональных исследований	основные методы шифрования в области защиты информации	использовать математические методы обработки и средства защиты информации	навыками построения систем защиты информации
2.	ПК-28	способность к инсталляции, отладке программных и настройке технических средств для ввода информационных систем в опытную и промышленную эксплуатацию	теоретические основы инсталляции и настройки программных и технических средств	организовывать ввод информационных систем в опытную и промышленную эксплуатацию	навыками инсталляции, отладки программных и настройке технических средств для ввода информационных систем в

					опытную и промышленную эксплуатацию
3.	ПК-34	способность к инсталляции, отладке программных и настройке технических средств для ввода информационных систем в опытную и промышленную эксплуатацию	теоретические основы инсталляции и настройки программных и технических средств	организовывать ввод информационных систем в опытную и промышленную эксплуатацию	навыками инсталляции, отладки программных и настройке технических средств для ввода информационных систем в опытную и промышленную эксплуатацию

Содержание и структура дисциплины (модуля)

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Вне аудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1.	Основы теории чисел	4	-	2	-	2
2.	Числовые сравнения	5	-	2	-	3
3.	Симметричные и ассиметричные шифры	5	-	2	-	3
4.	Методы взлома шифров	5	-	2	-	3
5.	Современные симметричные криптосистемы	5	-	2	-	3
6.	Отечественный стандарт шифрования данных ГОСТ	6	-	3	-	3
7.	Цифровая подпись	6	-	3	-	3
	Итого по дисциплине:	36	-	16	-	20

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

Основная литература:

1. Васильева, И.Н. Криптографические методы защиты информации: учебник и практикум для академического бакалавриата / И. Н. Васильева. - Москва: Юрайт, 2017. - 349 с. [Электронный ресурс]. - URL: - https://www.biblio-online.ru/book/59BABD78-5536-4ED4-BB9D-55E2F19F80B2

2. Лось, А. Б. Криптографические методы защиты информации: учебник для академического бакалавриата / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — М.: Издательство Юрайт, 2018. — 473 с. — (Серия: Бакалавр. Академический курс). — ISBN 978-5-534-01530-0. [Электронный ресурс]. - URL: - https://biblio-online.ru/book/27397D56-C8A1-4970-9F39-28E7FA40632A/

Автор (ы) РПД: профессор кафедры теоретической физики и компьютерных технологий
Тумаев Е.Н.