Аннотация к рабочей программы дисциплины

ФТД.03 «Информационная безопасность»

Объем трудоемкости: 2 зачетных единицы (72 часа (в 4 семестре), из них – 26 часов аудиторной нагрузки: лекционных 12 ч., практических 14 ч.; 43,8 часов самостоятельной работы, в том числе 2 ч. КСР, 0,2 ч. ИКР)

Цель дисциплины «Информационная безопасность» – ознакомление обучающихся с основными направлениями деятельности по обеспечению информационной безопасности и защите информации, рассмотрение аспектов нормативно-правовой базы, регламентирующей данную деятельность, задач руководителей, специалистов по сохранности информационных ресурсов, средств и механизмов, в том числе аппаратно-программных, используемых для этих целей, и, конечно, методов их применения.

Задачи дисциплины:

1. сформировать общее представление об информационной безопасности как о состоянии защищенности информационного ресурса сложной системы, понимание необходимости системного подхода к практической реализации такого состояния;
2. передать знания о порядке организации и практической реализации типовых мероприятий по обеспечению информационной безопасности и защите информации;
3. сформировать навыки анализа информационных ресурсов по следующим факторам: важность, конфиденциальность, уязвимость.

Место дисциплины в структуре ООП ВО:

Данная дисциплина относится к факультативной части блока ФТД «Факультативы» учебного плана. Дисциплина «Информационная безопасность» требует знаний по дисциплинам: системы искусственного интеллекта, анализ данных в профессиональной сфере и информатика и геоданные.

Курс необходим в качестве предшествующего для следующих дисциплин: «Картографическое обеспечение региональных исследований» и «Основы программирования в ГИС».

Требования к уровню освоения дисциплины

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

Код и наименование индикатора*	Результаты обучения по дисциплине
ОПК-4 Способен понимать принципы работы информационных технологий и решать стандартные задачи профессиональной деятельности с использованием информационно-коммуникационных технологий, в том числе технологии геоинформационных систем	
ИОПК-4.1. Понимает принципы работы информационных технологий	Знать источники возникновения информационных угроз; каналы утечки информации; направления и средства защиты информации; принципы национальной безопасности; исследования, ведущиеся в области информационной безопасности.
	Уметь применять правовые, организационные, технические и программные средства защиты информации; выявлять потенциальные каналы утечки информации и определять их характеристики; разрабатывать и обосновывать варианты эффективных управленческих решений в области информационной безопасности; систематизировать и обобщать информацию, готовить обзоры по вопросам информационной безопасности.
	Владеть навыками противодействия утечке

Код и наименование индикатора*	Результаты обучения по дисциплине
	компьютерной информации; навыками использования электронной цифровой подписи; навыками проведения аудита локальной политики безопасности, аудита доступа к объектам; специальной терминологией, применяемой в процессе защиты информации; навыками профессиональной аргументации при разборе стандартных ситуаций в сфере информационной безопасности
ИОПК-4.2. Решает стандартные задачи профессиональной деятельности с использованием информационно-коммуникационных технологий, в том числе технологии геоинформационных систем..	Знать порядок проведения анализа информационной безопасности объектов и систем
	Уметь проводить анализ информационной безопасности объектов информатизации.
	Владеть Навыками проведения анализа информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности.

Содержание дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
4 семестр						
1.	Введение в информационную безопасность	12	2	2		8
2.	Правовое обеспечение информационной безопасности	11	2	2		7
3.	Организационное обеспечение информационной безопасности	11	2	2		7
4.	Технические средства и методы защиты информации	12	2	2		8
5.	Программно-аппаратные средства и методы обеспечения информационной безопасности	12	2	2		8
6.	Криптографические методы защиты информации	14	2	4		8
	ИТОГО по разделам дисциплины	72	12	14	-	46
	Контроль самостоятельной работы (КСР)	2				
	Промежуточная аттестация (ИКР)	0,2				
	Подготовка к текущему контролю	-				
	Общая трудоемкость по дисциплине	72				

Курсовые работы: *не предусмотрены*
Форма проведения аттестации по дисциплине: зачет (4 семестр)

Автор (ы) РПД Кузякина М.В.