Аннотация
к рабочей программе дисциплины
ФТД.02 «Информационная безопасность»
(код и наименование дисциплины)

Объем трудоемкости: _2__ зачетные единицы

Цель дисциплины: Формирование у студентов знаний об основных направлениях исследований в области информационной безопасности, а также развития навыков применения актуальных цифровых методов, предназначенных для анализа состояния информационной безопасности социальных групп и образовательных организаций.

Задачи дисциплины:

Для достижения цели в ходе учебного процесса предполагается решить следующие задачи:

− познакомить студентов с современными теориями и концепциями информационного общества;

− выработать у студентов навыки сбора, систематизации и обработки информации, необходимой для выявления рисков информационной безопасности социальных групп и организаций, в том числе в учреждениях образования;

− развить способность проектирования индивидуального и (или) группового исследования с применением анализа данных для решения проблем информационной безопасности.

Место дисциплины (модуля) в структуре образовательной программы.

Дисциплина «Информационная безопасность» относится к части факультативных дисциплин учебного плана. Дисциплина рассчитана на слушателей без предварительной подготовки. Необходимо общее знакомство со спецификой профессиональной деятельности, а также знание иностранного языка на уровне, достаточном для изучения рекомендуемых источников.

Требования к уровню освоения дисциплины

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

Код и наименование индикатора	Результаты обучения по дисциплине
ОПК-9. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	
ОПК-9.4 Знание современных цифровых технологий, возможность их применения для цифровой безопасности, потенциальные риски и способы их нейтрализации.	***знает*** основные программные цифровые решения, необходимые для поддержания информационной безопасности общества и организаций, знает принципы работы современных информационных технологий
	умеет ориентироваться в программных цифровых решениях (в частности, в пакетах RStudio и библиотеках Python), позволяющих выявлять риски для информационной безопасности, умеет использовать цифровые технологии защиты информации
	владеет базовыми навыками программирования на языках R и Python, необходимыми для определения рисков и поддержания информационной безопасности, владеет навыками использования антивирусов и иных средств защиты информации, информационной гигиены и этикета.

Распределение трудоёмкости дисциплины по видам работ

Распределение видов учебной работы и их трудоемкости по разделам дисциплины. Разделы дисциплины, изучаемые в 6 семестре *(очная форма)*

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1.	Теоретические основания информационной безопасности. Классификация информационных угроз	10	2	2	-	6
2.	Риски информационного поля	10	2	2	-	6
3.	Законодательство в области информационной безопасности	12	2	4	-	6
4.	Способы обеспечения информационной безопасности. Индивидуальная и государственная защита информации	10	2	2	-	6
5.	Информационно-психологическая безопасность в цифровой среде	14	4	4	-	6
6.	Цифровые методы выявления рисков информационного поля	14	4	4		6
	Контроль самостоятельной работы (КСР)	2	-	-	-	-
	Промежуточная аттестация (ИКР)	0,8	-	-	-	-
	Итого по дисциплине:	72	16	18	-	36

Примечание: Л - лекции, ПЗ - практические занятия / семинары, ЛР - лабораторные занятия, СРС - самостоятельная работа студента

Курсовые работы: *не предусмотрены*

Форма проведения аттестации по дисциплине: *зачет*

Авторы: канд. соц. наук, доцент, Донцова М.В., канд. социол. наук, доцент Рунаев Т.А.