Аннотация к рабочей программы дисциплины
«Информационная безопасность»
(код и наименование дисциплины)

Объем трудоемкости: 2 зачетных единиц

Цель дисциплины: Формирование у студентов компетенций в области основных принципов, методов, способов и средств защиты информации, а также их применения в корпоративных информационно-технологических системах

Задачи дисциплины: 1) изучение и классификация причин нарушений безопасности, методов и средств защиты информации;

2) рассмотрение области применения и тенденций развития средств защиты информации;

3) приобретение практических навыков работы с современными сетевыми фильтрами и средствами криптографического преобразования информации, проектирование мониторов безопасности субъектов и объектов.

Место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность» относится к факультативным дисциплинам.

Требования к уровню освоения дисциплины

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

Код и наименование индикатора*	Результаты обучения по дисциплине
ПК-3 Способность проводить эффективный поиск, критически анализировать, интерпретировать и управлять информацией в цифровой среде с соблюдением принципов цифровой безопасности и кибергигиены.	
ПК-3.3 знание современных цифровых технологий, возможность их применения для цифровой безопасности, потенциальные риски, а также способы нейтрализации этих рисков, включая защиту от кибератак, вредоносного программного обеспечения, фишинга и других угроз, связанных с цифровым миром	Знать различных видов угроз, методы и инструменты защиты информации, стандарты и нормативные акты, подходы к управлению рисками, включая оценку уязвимостей, анализ угроз и разработку стратегий по минимизации рисков
	Уметь проводить анализ систем на наличие уязвимостей, использование инструментов для сканирования и тестирования на проникновение, отслеживать и анализировать новые угрозы в сфере кибербезопасности, проводить обучение и просвещение пользователей о безопасном поведении в сети, включа я распознавание фишинга и безопасное использование паролей
	Владеть навыками работы с современными инструментами и технологиями, такими как облачные решения, блокчейн, искусственный интеллект и машинное обучение для повышения уровня 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
1.	Тема 1. Актуальность информационной безопасности, понятия и определения	8	2	2		8
2.	Тема 2. Угрозы информации	8	2	2		8
3.	Тема 3. Организационно-правовая защита информации	16	4	4		8
4.	Тема 4. Программная защита информации	16	4	4		8
5.	Тема 5. Техническая защита информации	8	2	2		8
6.	Тема 6. Цифровая гигиена	8	2	2		5,8
	ИТОГО по разделам дисциплины	69,8	12	12		45,8
	Контроль самостоятельной работы (КСР)	2				
	Промежуточная аттестация (ИКР)	0,2				
	Подготовка к текущему контролю					
	Общая трудоемкость по дисциплине	72				

Курсовые работы: *(не предусмотрена)*
Форма проведения аттестации по дисциплине: (*зачет)*