

Аннотация к рабочей программе дисциплины
«ФТД.02 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»
(код и наименование дисциплины)

Объем трудоемкости: 2 зачетная единица (72 часов)

1 Цели и задачи изучения дисциплины.

1.1 Цель освоения дисциплины.

Цель преподавания данной дисциплины заключается в приобретении знаний и умений по информационной безопасности и защите информации в соответствии с государственным образовательным стандартом, в формировании у студентов знаний по анализу возможных каналов утечки информации, хранящейся в ЭВМ, передаваемой по информационным каналам, и методов защиты информации.

2. Задачи дисциплины

Изучение и усвоение следующих вопросов:

- разработка и анализ средств информационной безопасности информационных систем с обеспечением требований, вытекающих из документов, регламентирующих режим соблюдения государственной и коммерческой тайны;
- определение источников угроз безопасности информации в информационной системе;
- юридические основы правового обеспечения безопасности информационных систем;
- технические и программные средства обеспечения безопасности информационных систем;
- комплексная система защиты информации.

1.3 Место дисциплины в структуре образовательной программы.

Дисциплина «Информационная безопасность» относится к части, формируемой участниками образовательных отношений учебного плана ФТД. Факультативные дисциплины. В соответствии с рабочим учебным планом дисциплина изучается на 4 курсе по очной и на 4 курсе по очно-заочной форме обучения. Вид промежуточной аттестации: зачет.

Для успешного усвоения материала по дисциплине «Информационная безопасность» необходимо изучение дисциплин «Информационные технологии в юриспруденции», «Системы искусственного интеллекта».

1.4 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы.

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

Код и наименование индикатора*достижения компетенции	Результаты обучения по дисциплине
ОПК-9 Способен принимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	
ИОПК-9.1 Понимает принципы современных работ	ИОПК-9.1.1 Знает принципы и характер работы современных информационных работ

Код и наименование индикатора*достижения компетенции	Результаты обучения по дисциплине
информационных технологий.	технологий
ИОПК-9.2 Реализует принципы работы современных информационных технологий для решения задач профессиональной деятельности.	ИОПК-9.2.1 Умеет использовать современные информационные технологии для решения задач профессиональной деятельности

*Вид индекса индикатора соответствует учебному плану.

Результаты обучения по дисциплине достигаются в рамках осуществления всех видов контактной и самостоятельной работы обучающихся в соответствии с утвержденным учебным планом.

Индикаторы достижения компетенций считаются сформированными при достижении соответствующих им результатов обучения.

2.2 Содержание дисциплины:

Распределение видов учебной работы и их трудоемкости по темам дисциплины.

Темы дисциплины, изучаемые в 7 семестре (очная форма)

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Лек	ПР	Лаб	
1	2	3	4	5	6	7
1.	Введение. Цель и задачи дисциплины. Предмет и объект защиты информации. Понятие информационной безопасности.	8	2			6
2.	Наиболее распространенные угрозы. Анализ возможных каналов утечки информации.	10	2	2		6
3.	Неформальная модель нарушителя. Компьютерные преступления. Компьютерное пиратство. Хакеры.	8		2		6
4.	Анализ существующих подходов к обеспечению безопасности информации в информационных системах	6		2		4
5.	Отечественные и зарубежные стандарты в области информационной безопасности	6	2			4
6.	Юридические основы правового обеспечения безопасности информационных систем	6		2		4
7.	Административный уровень информационной безопасности. Управление рисками.	6		2		4
8.	Процедурный уровень информационной безопасности	6		2		4
9.	Методы идентификации и аутентификации пользователей	6		2		4
10.	Идентификация/аутентификация с помощью биометрических данных	9,8	2	2		5,8
	Итого по дисциплине:	71,8	8	16		47,8
	Контроль самостоятельной работы (КСР)		-	-	-	-
	Промежуточная аттестация (ИКР)	0,3	-	-	-	-
	Общая трудоемкость по дисциплине	72	-	-	-	-

Примечание: Лек – лекции, ПР – практические работы / семинары,

Темы дисциплины, изучаемые в 7 семестре (очно-заочная форма)

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Лек	ПР	Лаб	СР
1	2	3	4	5	6	7
11.	Введение. Цель и задачи дисциплины. Предмет и объект защиты информации. Понятие информационной безопасности.	10	2	2		6
12.	Наиболее распространенные угрозы. Анализ возможных каналов утечки информации.	8	2	2		4
13.	Неформальная модель нарушителя. Компьютерные преступления. Компьютерное пиратство. Хакеры.	6		2		4
14.	Анализ существующих подходов к обеспечению безопасности информации в информационных системах	6		2		4
15.	Отечественные и зарубежные стандарты в области информационной безопасности	8	2	2		4
16.	Юридические основы правового обеспечения безопасности информационных систем	6		2		4
17.	Административный уровень информационной безопасности. Управление рисками.	6		2		4
18.	Процедурный уровень информационной безопасности	6		2		4
19.	Методы идентификации и аутентификации пользователей	6		2		4
20.	Идентификация/аутентификация с помощью биометрических данных	9,8	2	2		5,8
	Итого по дисциплине:	71,8	8	20		43,8
	Контроль самостоятельной работы (КСР)		-	-	-	-
	Промежуточная аттестация (ИКР)	0,3	-	-	-	-
	Общая трудоемкость по дисциплине	72	-	-	-	-

Курсовые работы: не предусмотрены.

Форма проведения аттестации по дисциплине: зачет.

Автор Заикина Л.Н.