АННОТАЦИЯ ПРОГРАММЫ ДИСЦИПЛИНЫ

А1.В.ВД.2.1 «Информационная безопасность бизнеса и деятельности организации»

Общая трудоемкость изучения дисциплины составляет 3 ЗЕТ (108 часа)

1. Целями освоения дисциплины «Информационная безопасность бизнеса и деятельности организации» является формирование у аспирантов углубленных знаний о моделях и методах управления информационной безопасностью бизнеса (деятельности) организации

2**.** Дисциплина относится к дисциплинам по выбору вариативной части учебного плана ООП по направлению подготовки 10.06.01 – Информационная безопасность, направленности (профилю) «Методы и системы защиты информации, информационная безопасность».

Дисциплина предполагает наличие у аспирантов знаний по теории управления, теории принятия решений, общей теории управления и обеспечения информационной безопасности.

Знания и навыки, полученные аспирантами при изучении данной дисциплины, необходимы при изучении дисциплин:

– Методы и средства защиты информации в условиях информационного противоборства;

– Методы и системы защиты информации, информационная безопасность,

а также при подготовке к государственному экзамену, в научно-исследовательской деятельности и подготовке НКР (диссертации)

3. Компетенции обучающегося, формируемые в результате освоения дисциплины «Информационная безопасность бизнеса и деятельности организации»

Коды компетенции	Наименование компетенции	Структурные элементы компетенции (в результате освоения дисциплины обучающийся должен знать, уметь, владеть)
1	2	3
ОПК-1	Способность формулировать научные задачи в области обеспечения информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность	*Знать:* - компоненты моделей и методы управления информационной безопасностью бизнеса (деятельности); - основные источники рисков в информационной сфере организации, модели управления рисками
		Уметь: - определить компоненты модели информационной безопасности бизнеса (деятельности) в зависимости от целей бизнеса в информационной сфере и особенностей информационной сферы; - определить факторы рисков информационной безопасности бизнеса (деятельности) и сформировать факторную модель управления информационной безопасностью организации.
		Владеть: методологией рискориентированного подхода при анализе и исследовании системы управления информационной безопасности
ОПК-3	Способность обоснованно оце-	*Знать:*

	нивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности	- действующие нормативные документы в области управления информационной безопасностью; - модель процессов управления информационной безопасностью, их значимость и влияние на достижение целей информационной безопасности бизнеса (деятельности)
		Уметь: - определить процессы и подпроцессы управления информационной безопасностью бизнеса (деятельности) в зависимости от целей бизнеса в информационной сфере и особенностей информационной сферы; - выбирать модели и методы измерения и оценивания информационной безопасности в зависимости от целей бизнеса в информационной сфере и особенностей информационной сферы
		Владеть: навыками анализа и синтеза методов и моделей измерения и оценивания информационной безопасности в зависимости от целей бизнеса в информационной сфере и особенностей информационной сферы
ПК-4	Способность разрабатывать методы и модели информационной безопасности, проводить анализ защищенности и оценивать информационную безопасность объектов	*Знать:* - действующие нормативные документы в области оценки информационной безопасностью
		Уметь: - разрабатывать и выбирать модели и методы измерения и оценивания информационной безопасности в зависимости от целей бизнеса в информационной сфере и особенностей информационной сферы
		Владеть: навыками анализа и синтеза методов и моделей измерения и оценивания информационной безопасности в зависимости от целей бизнеса в информационной сфере и особенностей информационной сферы
ПК-5	Способность анализировать риски информационной безопасности, разрабатывать и применять современные методы и модели обеспечения информационной безопасности, оценки информационной безопасности автоматизированных систем	*Знать:* методы анализа и оценки рисков информационной безопасности автоматизированных систем
		Уметь: - разрабатывать модели информационной безопасности автоматизированных систем в зависимости от целей систем и их особенностей; - определить метод оценки информационной безопасности автоматизированных

		систем в зависимости от целей оценки и особенностей систем.
		Владеть: методиками оценки информационной безопасности автоматизированных систем
ПК-7	Способность создавать и исследовать модели систем защиты информации различного назначения, проводить анализ и обосновывать выбор решений по их применению	*Знать* модели управления информационной безопасностью систем различного назначения
		Уметь: - разрабатывать модели информационной безопасности автоматизированных систем в зависимости от назначения
		Владеть: методиками анализа и оценки информационной безопасности автоматизированных систем

Основные дидактические единицы: управление информационной безопасностью бизнеса; основные источники рисков в информационной сфере организации; факторы рисков информационной безопасности бизнеса (деятельности), модели управления рисками