

Аннотация к рабочей программе дисциплины

Автор: Полицук Ю.В

Наименование дисциплины: Б1.Б.18 Техническая защита информации

Цель освоения дисциплины:

- раскрыть основы правового регулирования отношений в информационной сфере, конституционные гарантии прав граждан на получение информации и механизм их реализации, понятия и виды защищаемой информации по законодательству РФ, систему защиты государственной тайны, основы правового регулирования отношений в области интеллектуальной собственности и способы защиты этой собственности, понятие и виды компьютерных преступлений, а также приобретение студентами знаний по организационному обеспечению защиты информации и формирование основных практических навыков работы в данной области.

1. Требования к результатам освоения дисциплины:

Индекс и содержание компетенции	Знания	Умения	Навыки и (или) опыт деятельности
ОК-5 способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	Этап 1 Цели, задачи, принципы и основные направления обеспечения технической защиты информации государства.	Этап 1 Проводить анализ и давать оценку степени защищенности компьютерных систем, осуществлять повышение уровня технических средств защиты информации	Этап 1 Профессиональной терминологией и методами теоретического обоснования в выборе технических средств обеспечения информационной безопасности
ОК-5 способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области	Этап 2 Современные подходы к обеспечению систем технической защиты информации и интересов личности, общества и государства	Этап 2 Применять отечественные и зарубежные стандарты в области обеспечения технической защиты информации, интересов личности, общества и государства	Этап 2 Владеть методологическим и принципами оценки технической защиты информации и защиты интересов личности, общества и государства

<p>обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики</p>			
<p>ПК-4 - способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты</p>	<p>Этап 1 Основные правила разработки политики безопасности организации. Компоненты политики безопасности</p>	<p>Этап 1 Умения разработки политики безопасности организации, согласно правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю;</p>	<p>Этап 1 Внедрения политики безопасности организации, согласно правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю; согласно правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю</p>
<p>ПК-4 - способностью участвовать в</p>	<p>Этап 2 Принципы и методы противодействия</p>	<p>Этап 2 Осуществлять меры противодействия</p>	<p>Этап 2 Навыки применения</p>

<p>работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты</p>	<p>несанкционированном у информационному воздействию на технические объекты</p>	<p>нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты.</p>	<p>комплексного подхода к обеспечению информационной безопасности объекта защиты</p>
<p>ПК-6 - Способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств в защите информации</p>	<p>Этап 1 Знание основных программно-аппаратных средств защиты информации</p>	<p>Этап 1 Умения настройки основных программно-аппаратных средств защиты информации</p>	<p>Этап 1 Навыки организации и проведения контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных</p>
	<p>Этап 2 Знание основных технических средств защиты информации</p>	<p>Этап 2 Умения работы с основными техническими средствами защиты информации</p>	<p>Этап 2 Навыки организации и проведения контрольных проверок работоспособности и эффективности применяемых технических средств защиты информации</p>
<p>ПК-11 - способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов</p>	<p>Этап 1 Основные понятия и методы теории вероятностей и математической статистики;</p>	<p>Этап 1 Умения проведения эксперимента в системах защиты информации</p>	<p>Этап 1 Навыки использовать математические методы и модели для решения прикладных задач.</p>
	<p>Этап 2 Математические методы обработки</p>	<p>Этап 2 Умения обработки оценки погрешности</p>	<p>Этап 2 Навыки обработки, оценки</p>

	экспериментальных данных.	и достоверности их результатов	погрешности и достоверности их результатов
ПК-12 - Способностью принимать участие в проведении экспериментальных исследований системы защиты информации	Этап 1 Основные понятия и методы теории вероятностей и математической статистики;	Этап 1 Умения проведения эксперимента в системах защиты информации	Этап 1 Навыки принимать участие в проведении экспериментальных исследований системы защиты информации
ПК-12 - Способностью принимать участие в проведении экспериментальных исследований системы защиты информации	Этап 2 Математические методы обработки экспериментальных данных.	Этап 2 Умения обработки результатов экспериментальных исследований системы защиты информации	Этап 2 Навыки формирования отчетности по результатам проведения экспериментальных исследований системы защиты информации

2. Содержание дисциплины:

Раздел 1 Основные понятия и определения.

Тема 1 Термины и определения в области технической защиты информации.

Тема 2 Классификация технических каналов утечки информации.

Раздел 2 Технические каналы утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами.

Тема 3 Общая характеристика и классификация технических каналов утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами.

Тема 4 Виды каналов утечки информации

Раздел 3 Системный подход к инженерно-технической защите информации.

Тема 5 Способы и средства защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами.

Тема 6 Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам.

Раздел 4 Основные этапы проектирования системы защиты информации техническими средствами.

Тема 7 Организация технической защиты информации.

Тема 8 Лицензирование деятельности по технической защите информации.

3. Общая трудоёмкость дисциплины: 3Е