

Аннотация к рабочей программе дисциплины

Автор Урбан В.А., доцент

Наименование дисциплины: Б2.В.02(П) Производственная эксплуатационная практика

Цель освоения дисциплины: комплексирование полученных теоретических знаний студентов в области комплексной защиты объектов информатизации с практической деятельностью.

1. Требования к результатам освоения дисциплины:

Индекс и содержание компетенций	Знания	Умения	Навыки и (или) опыт деятельности
ПК-1 - способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Этап 1: современные аппаратные средства вычислительной техники; Этап 2: современные инструментальные средства и технологии программирования	Этап 1: выполнять работы по настройке аппаратно - программных комплексов Этап 2: выполнять работы по настройке технических средств защиты информации	Этап 1: настройки и обслуживания аппаратно - программных комплексов Этап 2: настройки технических средств защиты информации
ПК-2 - способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Этап 1: основные программные средства для решения задач программирования Этап 2: современные специальные средства для решения задач программирования	Этап 1: разрабатывать программы прикладного значения Этап 2: разрабатывать программы специального значения	Этап 1: применения программных средств системного назначения Этап 2: применения программных средств специального назначения
ПК-3 - способностью администрировать подсистемы информационной безопасности объекта защиты	Этап 1: основные принципы администрирования Этап 2: современные инструментальные средства администрирования	Этап 1: проводить процедуру администрирования подсистемы безопасности Этап 2: уметь использовать инструментальные	Этап 1: навыками администрирования подсистемы безопасности Этап 2: навыками применения инструментальных средств

		средства администрирования подсистемы безопасности	администрирования подсистемы безопасности
ПК-4 - способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Этап 1: основные составляющие политики безопасности Этап 2: принципы разработки политики безопасности	Этап 1: разрабатывать политику безопасности Этап 2: применять комплексный подход к обеспечению информационной безопасности	Этап 1: навыки разработки политики безопасности Этап 2: применения комплексного подхода к обеспечению информационной безопасности
ПК-5 - способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	Этап 1: основные требования безопасности информации к объектам информатизации Этап 2: основные этапы аттестации объектов информатизации по требованиям безопасности информации	Этап 1: разрабатывать требования безопасности информации Этап 2: разрабатывать методику аттестации объектов информатизации	Этап 1: навыки формирования требований безопасности информации Этап 2: навыки в проведении аттестации объектов информатизации
ПК-6 - способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Этап 1: основные этапы контрольных проверок технических средств защиты информации Этап 2: основные принципы работы технических средств защиты информации	Этап 1: разрабатывать методику контрольных проверок технических средств защиты информации Этап 2: разрабатывать способы оценки эффективности применения программных, аппаратных средств защиты информации	Этап 1: навыками применения контрольных проверок Этап 2: навыками оценки эффективности применения аппаратно - программных комплексов
ПК-7 -	Этап 1: основные	Этап 1:	Этап 1: навыки

<p>способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений</p>	<p>этапы проектирования подсистемы информационной безопасности Этап 2: основные методы технико – экономического обоснования проектных решений</p>	<p>разрабатывать основные подсистемы безопасности информации Этап 2: проводить технико – экономическое обоснование проектных решений</p>	<p>разработки подсистем информационной безопасности Этап 2: навыки технико - экономического обоснования проектных решений</p>
<p>ПК-8 - способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов</p>	<p>Этап 1: основные этапы оформления рабочей документации Этап 2: основные нормативные и методические документы</p>	<p>Этап 1: разрабатывать основные рабочие документы Этап 2: применять нормативные документы в рабочей документации</p>	<p>Этап 1: навыки разработки рабочих документов Этап 2: навыки применения нормативных документов</p>
<p>ПК-10 - способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартам в области информационной безопасности</p>	<p>Этап 1: методику анализа информационной безопасности Этап 2: современные стандарты в области информационной безопасности</p>	<p>Этап 1: разрабатывать методику анализа информационной безопасности Этап 2: использовать стандарты в области информационной безопасности</p>	<p>Этап 1: разработки анализа информационной безопасности Этап 2: использования стандартов в области информационной безопасности</p>
<p>ПК-13 – способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности,</p>	<p>Этап 1: основные меры по выполнения обеспечения информационной безопасности Этап 2: основные меры поддержки обеспечения информационной безопасности</p>	<p>Этап 1: разрабатывать меры по обеспечению информационной безопасности Этап 2: разрабатывать меры поддержки по обеспечению информационной безопасности</p>	<p>Этап 1: разработки мер по обеспечению информационной безопасности Этап 2: разработки мер поддержки обеспечения информационной безопасности</p>

управлять процессом их реализации			
ПК-15 – способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Этап 1: основные компоненты технологического процесса защиты информации Этап 2: современные нормативные и методические документы в области информационной безопасности	Этап 1: организовывать технологический процесс защиты информации Этап 2: применять нормативные и методические документы в области информационной безопасности	Этап 1: организации технологического процесса защиты информации Этап 2: применения нормативных и методических документов в области информационной безопасности
ПСК-4.1 – способен учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации	Этап 1: основные информационные технологии Этап 2: автоматизированные системы, применяемые при организации защиты информации	Этап 1: разрабатывать и использовать особенности информационных технологий Этап 2: использовать особенности автоматизированных систем при организации системы защиты	Этап 1: использования информационных технологий при организации системы защиты Этап 2: навыки использования особенностей автоматизированных систем при организации системы защиты
ПСК-4.2 – способен выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем	Этап 1: основные операционные системы, системы управления базами данных Этап 2: комплекс задач при администрировании подсистем	Этап 1: выполнять комплекс задач администрирования подсистемы безопасности Этап 2: выполнять комплекс задач по безопасности операционных	Этап 1: выполнения комплекса задач администрирования подсистем безопасности Этап 2: выполнения администрирования компьютерных сетей по безопасности

управления базами данных, компьютерных сетей	информационной безопасности	систем и баз данных	
ПСК-4.3 – способен планировать и организовывать комплекс мероприятий по защите информации, связанных с обеспечением надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации	Этап 1: основные показатели надежности систем обеспечения информационной безопасности Этап 2: комплекс мер по обеспечению надежности систем обеспечения информационной безопасности	Этап 1: планировать комплекс мер по обеспечению надежности систем безопасности Этап 2: организовывать комплекс мер по обеспечению надежности подсистемы безопасности информации	Этап 1: планирования комплекса мер по обеспечению надежности систем безопасности Этап 2: организации комплекса мер по обеспечению надежности подсистемы безопасности информации

2. Содержание дисциплины:

Изучить теоретические аспекты построения технической охраны объекта.

Рассмотреть нормативно-правовые базы в области построения технической охраны.

Рассмотреть организационную структуру объекта.

Рассмотреть информационные потоки объекта.

Проанализировать возможные угрозы и каналы утечки конфиденциальной информации на объекте со стороны физической защиты.

Проанализировать существующую систему технической охраны

Выявить недостатки в системе технической охраны объекта.

3. Общая трудоёмкость дисциплины: 6 ЗЕ.