Аннотация к рабочей программе дисциплины

Автор Урбан В.А., доцент
Наименование дисциплины: Б2.В.03(Пд) Производственная (преддипломная) практика
Цель освоения дисциплины:
- углубление и закрепление знаний и умений, полученных студентом при теоретическом обучении в университете;
- расширение технического кругозора студента;
- приобретение студентом навыков инженерной работы по специальности;
- подготовка студента к самостоятельной инженерной деятельности;
- приобретение опыта организаторской и руководящей работы.

1. Требования к результатам освоения дисциплины:

Индекс и содержание компетенции	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	Этап1:- 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 средства	Этап 1: навыки администрирования подсистемы безопасности Этап 2: навыки применения инструментальных средств администрирования

		администрирования подсистемы безопасности	подсистемы безопасности
(ПК-4) способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Этап 1основные 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 2применения 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 в формирования требований безопасности информации Этап 2навыки 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: навыки применения контрольных проверок Этап 2: навыки оценки эффективности применении аппаратно - программных комплексов
(ПК-7) способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной	Этап 1: основные этапы проектирования подсистемы информационной безопасности Этап 2: основные	Этап 1: разрабатывать основные подсистемы безопасности информации Этап 2: проводить	Этап 1: навыки разработки подсистем информационной безопасности Этап 2: навыки технико -

безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	методы технико – экономического обоснования проектных решений	технико – экономическое обоснование проектных решений	экономического обоснования проектных решений
(ПК-8) способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	Этап 1: основные этапы оформления рабочей документации Этап 2: основные нормативные и методические документы	Этап 1: разрабатывать основные рабочие документы Этап 2: применять нормативные документы в рабочей документации	Этап 1: навыки разработки рабочих документов Этап 2: навыки применения нормативных документов
(ПК-9) способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	Этап 1: основные методы поиска научно – технической и нормативной литературы Этап 2: основные методические материалы по вопросам информационной безопасности	Этап 1: осуществлять подбор литературы по информационной безопасности Этап 2: уметь обобщать и составлять краткий обзор литературы по информационной безопасности	Этап 1: осуществления подбора литературы по информационной безопасности Этап 2: умения обобщения и составления обзора литературы по информационной безопасности
(ПК-10) способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Этап 1: методику анализа информационной безопасности Этап 2: современные стандарты в области информационной безопасности	Этап 1: разрабатывать методику анализа информационной безопасности Этап 2: использовать стандарты в области информационной безопасности	Этап 1: разработки анализа информационной безопасности Этап 2: использования стандартов в области информационной безопасности
(ПК-11) способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их	Этап 1: методику проведения экспериментов Этап 2: методику обработки, оценки результатов экспериментов	Этап 1: разрабатывать методику проведения экспериментов Этап 2: разрабатывать методику обработки	Этап 1: разработки методики проведения экспериментов Этап 2: разработки методики обработки и оценки

результатов		и оценки результатов эксперимента	результатов эксперимента
(ПК-12) способностью принимать участие в проведении экспериментальных исследований системы защиты информации	Этап 1: методику проведения экспериментов Этап 2: методику обработки, оценки результатов экспериментов	Этап 1: разрабатывать методику проведения экспериментов Этап 2: разрабатывать методику обработки и оценки результатов эксперимента	Этап 1: разработки методики проведения экспериментов Этап 2: разработки методики обработки и оценки результатов эксперимента
(ПК-13) способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Этап 1: основные меры по выполнения обеспечения информационной безопасности Этап 2: основные меры поддержки обеспечения информационной безопасности	Этап 1: разрабатывать меры по обеспечению информационной безопасности Этап 2: разрабатывать меры поддержки по обеспечению информационной безопасности	Этап 1: разработки мер по обеспечению информационной безопасности Этап 2: разработки мер поддержки обеспечения информационной безопасности
(ПК-14) способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности	Этап 1: основные меры по выполнения обеспечения информационной безопасности Этап 2: основные меры поддержки обеспечения информационной безопасности	Этап 1: разрабатывать меры по обеспечению информационной безопасности Этап 2: разрабатывать меры поддержки по обеспечению информационной безопасности	Этап 1: разработки мер по обеспечению информационной безопасности Этап 2: разработки мер поддержки обеспечения информационной безопасности
(ПК-15) способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами	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 2применения нормативных и методических документов в области информационной безопасности

Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю			
(ПСК4-1) 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
(ПСК4-2) способен выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей	Этап 1: основные операционные системы, системы управления базами данных Этап 2: комплекс задач при администрировании подсистем информационной безопасности	Этап 1: выполнять комплекс задач администрирования подсистемы безопасности Этап 2: выполнять комплекс задач по безопасности операционных систем и баз данных	Этап 1: выполения комплекса задач администрирования подсистем безопасности Этап 2: выполнения администрирования компьютерных сетей по безопасности
(ПСК4-3) 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
(ПСК4-4) способен участвовать в	Этап 1: основные этапы	Этап 1: разрабатывать	Этап 1: навыки разработки

разработке аппаратных и программных средств в составе автоматизированных систем, связанных с обеспечением информационной безопасности	проектирования подсистемы информационной безопасности Этап 2: основные методы технико – экономического обоснования проектных решений	основные подсистемы безопасности информации Этап 2: проводить технико – экономическое обоснование проектных решений	подсистем информационной безопасности Этап 2: навыки технико - экономического обоснования проектных решений

2. Содержание дисциплины:

Изучить теоретические аспекты организации технической защиты конфиденциальной информации на объекте.

Рассмотреть методики определения эффективности технической защиты конфиденциальной информации.

Рассмотреть организационную структуру объекта.

Рассмотреть информационные потоки объекта.

Проанализировать возможные угрозы и каналы утечки конфиденциальной информации по техническим каналам.

Проанализировать существующую систему технической защиты конфиденциальной информации.

Провести оценку эффективности системы технической защиты конфиденциальной информации.

3. Общая трудоёмкость дисциплины: 6 ЗЕ.