Аннотация к рабочей программе практики

Автор Боровский А.С., доцент
Наименование дисциплины: Б2.Б.04 (Пд) 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 осуществлять поиск, изучение, обобщениеисистематизацию научно-технической информации,нормативныхиметодическихматериаловв сфере профессиональнойдеятельности,втомчисленаиностранномязыке	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-2) - способностью создавать иисследоватьмоделиавтоматизированныхсистем	Этап 1: базовые понятия основ моделирования Этап 2:	Этап 1: использовать методы моделирования для создания	Этап 1: использования методов моделирования для создания

	модели автоматизированных систем	моделей Этап 2: использовать структурные модели	моделей Этап 2: использования структурных моделей
(ПК-3) - способностью проводить анализ защищенности автоматизированных систем	Этап 1: методику анализа защищенности автоматизированных систем Этап 2: современные стандарты в области информационной безопасности	Этап 1: разрабатывать методику анализа защищенности автоматизированных систем Этап 2: использовать стандарты в области информационной безопасности	Этап 1: разработки и анализа защищенности автоматизированных систем Этап 2: использования стандартов в области информационной безопасности
(ПК-4) - способностью разрабатыватьмоделиугрозимоделинарушителя информационнойбезопасностиавтоматизированнойсистемы	Этап 1основные модели угроз информационной безопасности Этап 2: модели нарушителей информационной безопасности	Этап 1: разрабатывать модели угроз информационной безопасности Этап 2: разрабатывать модели нарушителей информационной безопасности	Этап 1: разработки модели угроз информационной безопасности Этап 2: разработки модели нарушителей информационной безопасности

(ПК-5) - способностьюпроводитьанализ рисковинформационнойбезопасности автоматизированнойсистемы	Этап 1: основные риски информационной безопасности Этап 2: основные этапы анализа рисков информационной безопасности	Этап 1: рассчитывать риски информационной безопасности Этап 2: разрабатывать методику анализа рисков информационной безопасности	Этап 1: рассчета рисков информационной безопасности Этап 2 разработки методики анализа рисков информационной безопасности
(ПК-6) - способностьюпроводитьанализ,предлагатьи обосновыватьвыборрешенийпо обеспечениюэффективногоприменения автоматизированныхсистемв сфере профессиональнойдеятельности	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-7) - способностьюразрабатывать научно-техническуюдокументацию,готовить научно-технические отчеты, обзоры, публикациипорезультатамвыполненных работ	Этап 1: основные методы поиска научно – технической и нормативной	Этап 1: осуществлять подбор литературы по информационной безопасности	Этап 1: осуществления подбора литературы по информационной безопасно

	литературы Этап 2: основные методические материалы по вопросам информационной безопасности	Этап 2: уметь обобщать и составлять краткий обзор литературы по информационной безопасности	сти Этап 2: умения обобщения и составления обзора литературы по информационной безопасности
(ПК-8) - способностью разрабатывать и анализировать проектные решения по обеспечениюбезопасностиавтоматизированных систем	Этап 1: основные этапы проектирования подсистемы информационной безопасности Этап 2: основные методы технико – экономического обоснования проектных решений	Этап 1: разрабатывать основные подсистемы безопасности информации Этап 2: проводить технико – экономическое обоснование проектных решений	Этап 1: навыки разработки подсистем информационной безопасности Этап 2: навыки технико - экономического обоснования проектных решений
(ПК-9) - способностью участвовать в разработке защищенных автоматизированных системвсферепрофессиональнойдеятельности	Этап 1: основные этапы проектирования подсистемы информационной безопасности	Этап 1: разрабатывать основные подсистемы безопасности информации Этап 2:	Этап 1: навыки разработки подсистем информационной безопасности Этап 2: навыки

	Этап 2: основные методы технико – экономического обоснования проектных решений	проводить технико – экономическое обоснование проектных решений	технико - экономического обоснования проектных решений
(ПК-10) - способностьюприменятьзнанияв областиэлектроникиисхемотехники, технологий, методов и языковпрограммирования,технологий связи и передачи данныхпри разработкепрограммно-аппаратных компонентовзащищенных автоматизированных системвсферепрофессиональнойдеятельности	Этап 1: знать физические структуры и основные типы полупроводниковых приборов, их свойства и характеристики; Этап 2: знать принципы выбора элементной базы для функциональных узлов электронной аппаратуры с учетом требований эксплуатации и экономической эффективн	Этап 1: уметь работать с современной элементной базой электронной аппаратуры; Этап 2: уметь осуществлять обоснованный выбор структурных и принципиальных схем электронных устройств	Этап 1: владеть навыками чтения и составления принципиальных схем базовых функциональных узлов электронной аппаратуры; Этап 2: владеть навыками оценки параметров электронных приборов и устройств по комплекту документации

	ости		
(ПК-11) - способностьюразрабатыватьполитику информационнойбезопасности автоматизированной системы	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-12) - способностьюучаствоватьв проектированиисистемыуправления информационнойбезопасностьюавтоматизированной системы	Этап 1: основные этапы проектирования подсистемы информационной безопасности Этап 2: основные методы технико – экономического обоснования проектных решений	Этап 1: разрабатывать основные подсистемы безопасности информации Этап 2: проводить технико – экономическое обоснование проектных решений	Этап 1: навыки разработки подсистем информационной безопасности Этап 2: навыки технико - экономического обоснования проектных решений
(ПК-13) - способностьюучаствоватьв проектированиисредствзащитыинформации автоматизированной системы	Этап 1: основные этапы проектиро	Этап 1: разрабатывать основные	Этап 1: навыки разработки

	вания подсистемы информационной безопасности Этап 2: основные методы технико – экономического обоснования проектных решений	подсистемы безопасности информации Этап 2: проводить технико – экономическое обоснование проектных решений	подсистем информационной безопасности Этап 2: навыки технико - экономического обоснования проектных решений
(ПК-14) - способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических итехнических средств защитыинформации	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-15) - способностью участвовать впроведенииэкспериментально-исследовательских работприсертификации средствзащитыинформации автоматизированных систем	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-16) - способностьюучаствовать впроведении экспериментально-исследовательских работ при аттестации автоматизированных систем сучетом нормативных документовпозащитеинформации	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-17) - способностьюпроводитьинструментальныймониторинг защищенности информациивавтоматизированной системеи выявлятьканалыутечкиинформации	Этап 1: методику анализа информационной безопасности Этап 2: современн	Этап 1: разрабатывать методику анализа информационной безопасности	Этап 1: разработки анализа информационной безопасности Этап 2: использов

	ые стандарты в области информационной безопасности	Этап 2: использовать стандарты в области информационной безопасности	ания стандартов в области информационной безопасности
(ПК-18) - способностьюорганизовыватьработу малыхколлективовисполнителей, вырабатыватьиреализовывать управленческие решениявсферепрофессиональной 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-19) - способностьюразрабатыватьпредложения по совершенствованиюсистемы управленияинформационной безопасностьюавтоматизированной системы	Этап 1: основные меры по выполнения обеспечения информационной безопасности Этап 2: основные меры	Этап 1: разрабатывать меры по обеспечению информационной безопасности Этап 2: разрабатывать меры поддержк	Этап 1: разработки мер по обеспечению информационной безопасности Этап 2: разработки мер поддержки

	поддержки обеспечения информационной безопасности	и по обеспечению информационной безопасности	обеспечения информационной безопасности
(ПК-20) - способностью организовать разработку, внедрение, эксплуатацию и сопровождениеавтоматизированной системыс учетомтребованийинформационной безопасности	Этап 1: принципы разработки и внедрения информационных систем; Этап 2: принципы эффективного применения автоматизированных информационных систем с учетом требований информационной безопасности	Этап 1: использовать методы разработки и внедрения информационных систем Этап 2: реализовать разработку автоматизированной информационной системы с учетом требований информационной безопасности	Этап 1: методами разработки, внедрения, эксплуатации информационных систем Этап 2: методами сопровождения информационных систем
(ПК-21) - способностью разрабатывать проектыдокументов, регламентирующих работу по обеспечениюинформационнойбезопасности автоматизированныхсистем	Этап 1: основные этапы оформления рабочей документации Этап 2: основные	Этап 1: разрабатывать основные рабочие документы Этап 2: применять нормативн	Этап 1: навыки разработки рабочих документов Этап 2: навыки применения

	нормативные и методические документы	ые документы в рабочей документации	нормативных документов
(ПК-22) - способностьюучаствоватьв формированииполитикиинформационной безопасностиорганизациииконтролироватьэффективностьеереализации	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-23) - способностьюформироватькомплексмер (правила,процедуры,методы)для защитыинформациииограниченногодоступа	Этап 1: основные принципы администрирования Этап 2: современные инструментальные средства администрирования	Этап 1: проводить процедуру администрирования подсистемы безопасности Этап 2: уметь использовать инструментальные средства администрирования подсистемы	Этап 1: навыки администрирования подсистемы безопасности Этап 2: навыки применения инструментальных средств администрирования подсистемы безопасно

		безопасности	сти
(ПК-24) - способностью обеспечить эффективное применениеинформационно-технологических ресурсов автоматизированной системы с учетомтребований информационнойбезопасности	Этап 1: принципы эффективного применения информационно-технологических ресурсов; Этап 2: принципы информационной безопасности	Этап 1: использовать методы эффективного применения информационно-технологических ресурсов Этап 2: реализовать политику информационной безопасности	Этап 1: методами разработки, внедрения, эксплуатации информационно-технологических ресурсов Этап 2: методами сопровождения информационно-технологических ресурсов
(ПК-25) - способностьюобеспечитьэффективноеприменениесредств защиты информационно-технологических ресурсовавтоматизированной системыи восстановлениеих работоспособности при возникновении нештатных ситуаций	Этап 1: принципы эффективной реализации резервного копирования данных; Этап 2: принципы информационной безопасности в процессах резервного копирован	Этап 1: использовать методы резервного копирования данных Этап 2: реализовать политики информационной безопасности для процессов резервного копирования данных	Этап 1: методами разработки, внедрения, эксплуатации резервного копирования данных Этап 2: методами сопровождения резервного копирования данных

	ия данных		
(ПК-26) - способностьюадминистрироватьподсистему информационнойбезопасности автоматизированной системы	Этап 1: основные принципы администрирования Этап 2: современные инструментальные средства администрирования	Этап 1: проводить процедуру администрирования подсистемы безопасности Этап 2: уметь использовать инструментальные средства администрирования подсистемы безопасности	Этап 1: навыки администрирования подсистемы безопасности Этап 2: навыки применения инструментальных средств администрирования подсистемы безопасности
(ПК-27) - способностьювыполнятьполныйобъемработ,связанныхсреализациейчастных политикинформационной безопасностиавтоматизированной системы,осуществлять мониторингиаудитбезопасностиавтоматизированнойсистемы	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-28) - способностьюуправлять информационнойбезопасностьюавтоматизированной системы	Этап 1: основные меры по выполнения обеспечения информационной безопасности Этап 2: основные меры поддержки и 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 и обеспечения информационной безопасности
(ПСК-3.1) - способностью проводить оценкуэффективности средствзащитыинформации, использующихсянакритическиважныхобъектахив автоматизированных системах критическиважныхобъектов	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	Этап 1: использования информационных технологий при организации системы защиты Этап 2: навыки использования особенностей автоматизированных систем при организации

		защиты	системы защиты
(ПСК-3.2) - способностью участвовать в разработке, осуществлять внедрение и эксплуатациюсредствзащитыинформации,использующихсянакритически важных объектахивавтоматизированныхсистемахкритическиважныхобъектов	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
(ПСК-3.3) - способностью применять современнуюнормативнуюбазу,регламентирующую деятельностькритическиважныхобъектови обеспечениеинформационной безопасности критически важных объектов и автоматизированных систем критическиважныхобъектов	Этап 1: основные показатели надежности систем обеспечения информационной безопасности Этап 2: комплекс мер по обеспечению надежности систем обеспечения информац	Этап 1: планировать комплекс мер по обеспечению надежности систем безопасности Этап 2:организовывать комплекс мер по обеспечению надежности подсистемы	Этап 1: планирования комплекса мер по обеспечению надежности систем безопасности Этап 2: организации комплекса мер по обеспечению надежности подсистемы

	ионной безопасности	безопасности информации	безопасности информации
(ПСК-3.4) - способностьюразрабатыватьтехнические регламентыдля различныхвидов деятельностипо обеспечениюинформационнойбезопасности критическиважных объектовиавтоматизированных системкритическиважныхобъектов	Этап 1: основные этапы проектирования подсистемы информационной безопасности Этап 2: основные методы технико – экономического обоснования проектных решений	Этап 1: разрабатывать основные подсистемы безопасности информации Этап 2: проводить технико – экономическое обоснование проектных решений	Этап 1: навыки разработки подсистем информационной безопасности Этап 2: навыки технико - экономического обоснования проектных решений
(ПСК-3.5) - способностью проектировать, внедрять ииспользовать системы мониторинга средствзащитыинформации, функционирующих накритическиважныхобъектахи вавтоматизированных системахкритическиважныхобъектов	Этап 1: основные меры по выполнения обеспечения информационной безопасности Этап 2: основные меры поддержки обеспечения информационной	Этап 1: разрабатывать меры по обеспечению информационной безопасности Этап 2: разрабатывать меры поддержки по обеспечению информационной безопасно	Этап 1: разработки мер по обеспечению информационной безопасности Этап 2: разработки мер поддержки обеспечения информационной безопасности

	безопасности	сти	

2. Содержание дисциплины:

Распределение по разделам/этапам практики, видам работ, форм текущего контроля с указанием номера осваиваемой компетенции в соответствии с ОПОП - Не предусмотрено

3. Общая трудоёмкость дисциплины: _18_ ЗЕ.