

ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ
КАФЕДРА СТРАТЕГИЧЕСКИХ ИНФОРМАЦИОННЫХ ИССЛЕДОВАНИЙ

ОДОБРЕНО УМС ИИКС

Протокол № УМС-575/01-1

от 30.08.2021 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
ПРОИЗВОДСТВЕННАЯ ПРАКТИКА (ПРЕДДИПЛОМНАЯ)

Направление подготовки
(специальность)

[1] 10.04.01 Информационная безопасность

Наименование образовательной
программы (специализация)

Обеспечение безопасности значимых объектов
критической информационной инфраструктуры

Семестр	Трудоемкость, кред.	Общий объем курса, час.	Практич. занятия, час.	В форме практической подготовки/ В	СРС, час.	Форма(ы) контроля, экз./зач./КР/КП
4	9	324	324		0	
Итого	9	324	324	0	0	Э

АННОТАЦИЯ

Преддипломная практика студента является обязательным разделом основной образовательной программы магистратуры. Она представляет собой вид учебных занятий, непосредственно ориентированных на профессионально-практическую подготовку обучающихся. Результаты практики являются основной частью выпускной квалификационной работы, которая в соответствии с программой выполняется в период выполнения научно-исследовательской работы и прохождения практики. Рабочая программа практики содержит описание целей ее освоения, ее место в структуре образовательной программы, формируемые в результате выполнения компетенции студента, структуру и содержание практики, используемые во время выполнения практики образовательные технологии и иное обеспечение.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целью практики является: закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин общенаучного модуля и профессионального модуля, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки студента; изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; изучение источников информации и системы оценок эффективности применяемых мер защиты информации; подготовка студента к решению задач комплексного обеспечения информационной безопасности предприятия (объекта защиты), задач, связанных с информационной безопасностью объектов информатизации и к выполнению выпускной квалификационной работы.

В ходе практики студент решает следующие задачи:
изучает:

- документацию, патентные и литературные источники в целях их использования при выполнении выпускной квалификационной работы;
- назначение, состав, принцип функционирования или организации объекта исследования или разработки;

выполняет:

- сравнительный анализ возможных вариантов проведения исследования и решения поставленной задачи в соответствии с тематикой дипломной работы;
- анализ необходимых мероприятий по безопасности жизнедеятельности, обеспечению экологической чистоты, защите интеллектуальной собственности;
- сбор материалов для всех разделов выпускной квалификационной работы.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Преддипломная практика выполняется в течение 6 недель в 5-м учебном семестре.

Преддипломная практика является неотъемлемым этапом подготовки выпускной квалификационной работы, диссертации магистра.

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
УКЦ-1 [1] – Способен решать исследовательские, научно-технические и производственные задачи в условиях неопределенности, в том числе выстраивать деловую коммуникацию и организовывать работу команды с использованием цифровых ресурсов и технологий в цифровой среде	3-УКЦ-1 [1] – Знать современные цифровые технологии, используемые для выстраивания деловой коммуникации и организации индивидуальной и командной работы У-УКЦ-1 [1] – Уметь подбирать наиболее релевантные цифровые решения для достижения поставленных целей и задач, в том числе в условиях неопределенности В-УКЦ-1 [1] – Владеть навыками решения исследовательских, научно-технических и производственных задач с использованием цифровых технологий
УКЦ-2 [1] – Способен к самообучению, самоактуализации и саморазвитию с использованием различных цифровых технологий в условиях их непрерывного совершенствования	3-УКЦ-2 [1] – Знать основные цифровые платформы, технологи и интернет ресурсы используемые при онлайн обучении У-УКЦ-2 [1] – Уметь использовать различные цифровые технологии для организации обучения В-УКЦ-2 [1] – Владеть навыками самообучения, самоактуализации и саморазвития с использованием различных цифровых технологий

Профессиональные компетенции в соответствии с задачами и объектами (областями знаний) профессиональной деятельности:

Задача профессиональной деятельности (ЗПД)	Объект или область знания	Код и наименование профессиональной компетенции; Основание (профессиональный стандарт-ПС, анализ опыта)	Код и наименование индикатора достижения профессиональной компетенции
проектный			
Проектирование систем обеспечения информационной безопасности (СОИБ) конкретных объектов на стадиях разработки, эксплуатации и модернизации	Средства и технологии обеспечения безопасности значимых объектов критической информационной инфраструктуры	ПК-2.1 [1] - Способен определять объекты КИИ, готовить перечни объектов КИИ, подлежащие категорированию <i>Основание:</i> Профессиональный стандарт: 06.030, 06.034	3-ПК-2.1[1] - Знать: Основные принципы выявления объектов КИИ, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов; Принципы построения АСУ ТП АЭС и

			<p>критические процессы, происходящие в результате штатной работы. ; У-ПК-2.1[1] - Уметь: Выявлять и собирать сведения о критических процессах в АСУ, информационных и телекоммуникационных системах, в частности в АСУ ТП АЭС; Определять категории значимости объектов КИИ; Формировать сведения о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий. ; В-ПК-2.1[1] - Владеть: Навыком определения критических процессов в АСУ, информационных и телекоммуникационных системах, в частности в АСУ ТП АЭС; Навыком определения категории значимости объектов КИИ; Навыком формирования сведения о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий.</p>
<p>Проектирование систем обеспечения информационной безопасности (СОИБ) конкретных объектов на стадиях разработки, эксплуатации и модернизации</p>	<p>Средства и технологии обеспечения безопасности значимых объектов критической информационной инфраструктуры</p>	<p>ПК-2.2 [1] - Способен осуществлять категорирование объектов КИИ и готовить сведения о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости</p>	<p>З-ПК-2.2[1] - Знать: Процедуру категорирования объектов КИИ, в том числе порядок создания комиссии по категорированию, порядок определения категорий значимости объектов КИИ; Последствия инцидентов</p>

		<p>присвоения ему одной из таких категорий</p> <p><i>Основание:</i> Профессиональный стандарт: 06.030, 06.032</p>	<p>информационной и ядерной безопасности; Процедуру подготовки и направления в ФСТЭК России сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий. ; У-ПК-2.2[1] - Уметь: Разрабатывать необходимые документы, содержащие сведения о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий для направления в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности КИИ, по утвержденной им форме. ; В-ПК-2.2[1] - Владеть: Навыком анализа последствий инцидентов информационной и ядерной безопасности; Навыком категорирования объектов КИИ.</p>
<p>Проектирование систем обеспечения информационной безопасности (СОИБ) конкретных объектов на стадиях разработки, эксплуатации и модернизации</p>	<p>Средства и технологии обеспечения безопасности значимых объектов критической информационной инфраструктуры</p>	<p>ПК-2.3 [1] - Способен устанавливать требования к обеспечению безопасности значимого объекта КИИ, осуществлять выбор и реализацию мер по обеспечению безопасности значимых объектов КИИ</p>	<p>3-ПК-2.3[1] - Знать: Отечественные стандарты в области информатизации и обеспечения информационной безопасности АСУ, информационных и телекоммуникационных систем общего и специального назначения; Основные принципы обеспечения</p>

		<p><i>Основание:</i> Профессиональный стандарт: 06.033, 06.034</p>	<p>безопасности КИИ; Основные положения ядерной безопасности; Причины возникновения инцидентов ядерной безопасности; Основные виды угроз для АСУ ТП на АЭС; Сущность основных физических процессов и информационных угроз в АСУ ТП в ядерном реакторе, их взаимосвязь; Требования по обеспечению безопасности значимых объектов КИИ.; У-ПК-2.3[1] - Уметь: Планировать, разрабатывать, совершенствовать и осуществлять внедрение мероприятий, регламентирующих правила и процедуры по обеспечению безопасности значимых объектов КИИ; Выявлять основные информационные угрозы в АСУ ТП ядерного реактора; Проводить оценку необходимости применения средств ядерной защиты реакторов. ; В-ПК-2.3[1] - Владеть: Навыками внедрения мероприятий, регламентирующих правила и процедуры по обеспечению безопасности значимых объектов КИИ; Навыками внедрения мероприятий по реализации комплекса мер, направленных на предотвращение, отражение и нейтрализацию угроз информационной</p>
--	--	---	---

			<p>безопасности значимых объектов КИИ; Навыком обоснованного выбора средств защиты информации и средств ядерной защиты реакторов с учетом их стоимости, совместимости с применяемыми программными и программно-аппаратными средствами, функций безопасности этих средств и особенностей их реализации, а также категории значимого объекта КИИ; Навыком общего/детального анализа структуры системы безопасности значимого объекта КИИ.</p>
<p>организационно-управленческий</p>			
<p>Организация работы коллектива исполнителей, принятие управленческих решений в условиях спектра мнений, определение порядка выполнения работ; Разработка проектов организационно-распорядительных документов в области обеспечения безопасности значимых объектов критической информационной инфраструктуры</p>	<p>Контроль защищенности информации на объектах информатизации</p>	<p>ПК-2.4 [1] - Способен обеспечивать безопасность значимого объекта КИИ на всех стадиях жизненного цикла</p> <p><i>Основание:</i> Профессиональный стандарт: 06.031, 06.033, 06.034</p>	<p>З-ПК-2.4[1] - Знать: Принципы организации систем безопасности значимых объектов КИИ и обеспечения их функционирования; Критерии обеспечения ядерной безопасности значимых объектов КИИ.;</p> <p>У-ПК-2.4[1] - Уметь: Анализировать данные, получаемые при использовании средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, в том числе информации о наличии в сетях электросвязи, используемых для организации взаимодействия объектов критической</p>

			<p>информационной инфраструктуры, признаков компьютерных атак.; В-ПК-2.4[1] - Владеть: Навыком проведения перспективных исследований в области информационной безопасности и ядерной защиты объектов КИИ; Навыком совершенствования системы безопасности значимых объектов КИИ; Навыком управления (администрирования) системой безопасности и реагирования на компьютерные инциденты; Навыком проведения контроля состояния (мониторинг) критических процессов и системы безопасности значимого объекта КИИ.</p>
--	--	--	---

4. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Разделы учебной дисциплины, их объем, сроки изучения и формы контроля:

№ п.п	Наименование раздела учебной дисциплины	Недели	Лекции/ Практи. (семинары) / Лабораторные работы, час.	Обязат. текущий контроль (форма*, неделя)	Максимальный балл за раздел**	Аттестация раздела (форма*, неделя)	Индикаторы освоения компетенции
	<i>4 Семестр</i>						
1	Выполнение практического задания, подготовка отчёта, защита практики	1-6	0/324/0		50	Отч-9	З-ПК-2.1, У-ПК-2.1, В-ПК-2.1, 3-ПК-2.2, У-ПК-2.2,

							В-ПК-2.2, 3-ПК-2.3, У-ПК-2.3, В-ПК-2.3, 3-ПК-2.4, У-ПК-2.4, В-ПК-2.4, 3-УКЦ-1, У-УКЦ-1, В-УКЦ-1, 3-УКЦ-2, У-УКЦ-2, В-УКЦ-2
	<i>Итого за 4 Семестр</i>		0/324/0		50		
	Контрольные мероприятия за 4 Семестр				50	Э	3-ПК-2.1, У-ПК-2.1, В-ПК-2.1, 3-ПК-2.2, У-ПК-2.2, В-

							ПК-2.2, 3-ПК-2.3, У-ПК-2.3, В-ПК-2.3, 3-ПК-2.4, У-ПК-2.4, В-ПК-2.4, 3-УКЦ-1, У-УКЦ-1, В-УКЦ-1, 3-УКЦ-2, У-УКЦ-2, В-УКЦ-2
--	--	--	--	--	--	--	--

* – сокращенное наименование формы контроля

** – сумма максимальных баллов должна быть равна 100 за семестр, включая зачет и (или) экзамен

Сокращение наименований форм текущего контроля и аттестации разделов:

Обозначение	Полное наименование
ЗО	Зачет с оценкой
Отч	Отчет

КАЛЕНДАРНЫЙ ПЛАН

Недел	Темы занятий / Содержание	Лек.,	Пр./сем.	Лаб.,
-------	---------------------------	-------	----------	-------

и		час.	, час.	час.
	<i>4 Семестр</i>	0	324	0
1-6	Выполнение практического задания, подготовка отчёта, защита практики	0	324	0
1 - 4	Постановка задачи и выполнение работы Согласование с руководителем и консультантом задания на практику. Инструктаж по технике безопасности. те здесь подробное описание пункта.Выполнение практического задания по месту прохождения практики	Всего аудиторных часов		
		0	144	0
		Онлайн		
		0	0	0
5 - 8	Выполнение работы Выполнение практического задания по месту прохождения практики	Всего аудиторных часов		
		0	144	0
		Онлайн		
		0	0	0
9	Подготовка отчета, защита практики Оформление отчёта о практике. Подготовка доклада и презентации. Защита результатов практики перед комиссией кафедры.	Всего аудиторных часов		
		0	36	0
		Онлайн		
		0	0	0

Сокращенные наименования онлайн опций:

Обозна- чение	Полное наименование
ЭК	Электронный курс
ПМ	Полнотекстовый материал
ПЛ	Полнотекстовые лекции
ВМ	Видео-материалы
АМ	Аудио-материалы
Прз	Презентации
Т	Тесты
ЭСМ	Электронные справочные материалы
ИС	Интерактивный сайт

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Цель прохождения преддипломной практики достигается сочетанием применения традиционных и инновационных педагогических технологий, направленных на развитие познавательной активности, творческой самостоятельности студентов. Последовательное и целенаправленное выдвижение перед студентом познавательных задач, решая которые студенты активно усваивают знания. Поисковые методы; постановка познавательных задач.

Самостоятельная работа студентов подразумевает под собой проработку различного материала и выполнения задания в форме решения поставленных задач. Для контроля усвоения студентом разделов данной практики используются отчетные материалы выполненного исследования в соответствии с заданиями.

Производственное оборудование

1. Измерительная площадка (альтернативная).

По адресу: 115409, г. Москва, Каширское шоссе, д. 31, кор. Т, пом. Т-215

Контрольно-измерительное и испытательное оборудование

1. Измерительная антенна дипольная активная АИ5-0 с УР-1.6 Россия 943 / 01869 9 кГц...2 ГГц
2. Измерительная антенна рамочная активная АИР3-2 с УР-1.6 Россия 01883 / 01890 0,009 – 30 МГц
3. Измерительная антенна дипольная активная АИ5-0 с УР-1.6 Россия 1650 / 03773 9 кГц...2 ГГц
4. Антенна измерительная рамочная АИР3-2 с УР-1.6 Россия 03806 / 03772 0,009 – 30 МГц
5. Антенна измерительная рупорная П6-59 Россия 301 1,0 – 18 ГГц
6. Токосъемник измерительный ТИ2-3 0574 0,01...300 МГц
7. Пробник напряжения Я6-122/1 282 0,01...300 МГц
8. Широкополосная дисконусная антенна ДА-3000 Инв. 43-015 26 МГц...2ГГц
9. Автоматизированная система (программно-аппаратный комплекс) оценки защищённости технических средств от утечки информации по каналу побочных электромагнитных излучений и наводок Сигурд-М2 ООО «ЦБИ «МАСКОМ» Россия 168 0,9 кГц – 13,2 ГГц
10. Система оценки защищённости выделенных помещений по виброакустическому каналу Шепот ООО «ЦБИ «МАСКОМ» Россия 0164 20 Гц...7 кГц
11. Калибратор акустический CAL200 Larson&Davis США 5903 20 Гц...7 кГц
12. Калибратор акустический CAL200 Larson&Davis США 9309 20 Гц...7 кГц
13. Генератор тестового акустического сигнала ШОРОХ-2МИ ООО «ЦБИ «МАСКОМ» Россия МИ222-08 20 Гц...7 кГц
14. Активные стереоколонки Microlab PRO 3 Китай Инв. 43-211 40 Гц...24 кГц
15. Генератор радиосигналов программируемый G3900H Россия G015 НЧ 9 кГц...30 МГц ВЧ 30 МГц...3 ГГц
16. Универсальная экранированная колонка УЭК МСШЕ.657350.001 ГР256-08 125 Гц...10 кГц
17. Универсальная экранированная колонка УЭК ООО «ЦБИ «МАСКОМ» Россия ГР576-11 125 Гц...10 кГц
18. Дополнительный модуль к автоматизированным системам оценки защищенности технических средств от утечки информации по каналу ПЭМИН серии «Сигурд» Модуль «ЦОС» МК-14 ООО «ЦБИ «МАСКОМ» Россия 0009 0,01 - 30 МГц
19. Анализатор спектра R&S ESPI 3 102013 9 кГц – 3 ГГц
20. Анализатор спектра IFR 2394A I07093005 9 кГц – 3 ГГц
21. Осциллограф С1-137М 090028 0 – 30 МГц
22. Осциллограф С1-72 629278 0 – 10 МГц
23. Осциллограф двухлучевой универсальный С1-74 2173 50 МГц
24. Источник питания постоянного тока Б5-47 12263 Величина выходного напряжения 0,1-29,9 В Ток нагрузки 0,01-2,99 А
25. Автоматизированная система исследования эффекта акустоэлектрических преобразований в технических средствах и отходящих от них линиях ТАЛИС ООО «ЦБИ «МАСКОМ» Россия 0019 10 кГц - 7,26 ГГц
26. Система автоматизированная измерительная для измерения электрических сигналов, возникающих за счет АЭП в ТС ТАЛИС-НЧ-М1 ООО «ЦБИ «МАСКОМ» Россия 0009 100 Гц - 10 кГц

Средства защиты информации

1. Комплекс средств защиты информации от несанкционированного доступа Защита информации от несанкционированного доступа СЗИ НСД «Аккорд-NT/2000» v.3.0. ЗАО «ОКБ САПР»
2. Генератор шума Маскировка информативных ПЭМИ ОТСС ГШ-1000М; Изготовитель: ФГУП СКБ ИРЭ РАН
3. Генератор шума Маскировка информативных ПЭМИ ОТСС в диапазоне 0,1-2000 МГц, ГШ-2500; Изготовитель: ФГУП СКБ ИРЭ РАН
4. Генератор шума Техническое СЗИ, обработ-ой на объектах 1,2 и 3 категорий от утечки за счёт наводок инф. Сигналов в линии электропитания и заземления «Соната-РС1»; Изготовитель: ЗАО «АННА»
5. Защитное устройство Фильтр сетевой помехоподавляющий Защита радиоэлектронных устройств и СВТ от утечки информации по цепям электропитания ФСП-1Ф-7А; ОАО «Приборостроитель», Россия
2007 Собственность Сертификат ФСТЭК №148/2 до 01.04.2016 г.
6. Защитное устройство Фильтр сетевой помехоподавляющий комбинированный Защита радиоэлектронных устройств и СВТ от утечки информации по цепям электропитания на ток 10А ФСПК-10-220-99-УХЛ4; ООО НПП «ЭЛКОМ»
7. Сетевой генератор шума Защита объектов информатизации от утечки информации по цепям электропитания ЛГШ-221; ООО «Ленспецпроизводство»
8. Генератор шума Система активной защиты от утечки информации по каналам ПЭМИН ЛГШ-501; ООО «Ленспецпроизводство»
9. Устройство защиты объектов информатизации от утечки по техническим каналам Защита объектов информатизации от утечки информации по цепям электропитания на объектах до 1 кат. Соната-Р2; ЗАО «АННА»
10. Устройство защиты Защита громкоговорителя системы оповещения от утечки акустических сигналов помещения МП-5; ООО «РЕНОМ»
11. Устройство комбинированной защиты объектов информатизации для активной защиты объектов информатизации от утечки в форме информативных электрических сигналов и наводок по сети электропитания, заземления, коммуникациям за счёт ПЭМИН Соната РК1
12. Устройство защиты телефонных линий Защиты ТА цифровых линий от утечки речевой информации в режиме ожидания МП-1Ц; ООО «РЕНОМ», Россия
13. Устройство защиты телефонных линий Защиты ТА аналоговых линий от утечки речевой информации в режиме ожидания МП-1А; ООО «РЕНОМ», Россия
14. Программа поиска информации на дисках Программа для поиска информации на дисках TERRIER-3.0; ЗАО «ЦБИ-сервис», Россия
15. Анализатор уязвимостей СЗИ СВТ от НСД Программа для анализа уязвимостей средств защиты СВТ от НСД Ревизор-1 ХР; ЗАО «ЦБИ-сервис», Россия
16. Анализатор уязвимостей СЗИ СВТ от НСД Программа для анализа уязвимостей средств защиты СВТ от НСД Ревизор-2 ХР; ЗАО «ЦБИ-сервис», Россия
17. Программа фиксации и контроля исходного состояния программ Программа фиксации и контроля исходного состояния программного комплекса «ФИКС» (версия 2.0.1), является программным средством контроля эффективности применения СЗИ – по 3 уровню НДВ ФИКС 2.0.1; ЗАО «ЦБИ-сервис», Россия

18. Программа для фиксации и контроля исходного состояния программного комплекса Программа фиксации и контроля исходного состояния программного комплекса «ФИКС» (версия 2.0.2), является программным средством контроля эффективности применения СЗИ – по 2 уровню НДВ ФИКС 2.0.2; ЗАО «ЦБИ-сервис», Россия

19. Программа фиксации и контроля целостности информации Программа фиксации и контроля целостности информации «ФИКС-UNIX 1.0» - по 2 уровню контроля для НДВ ФИКС-UNIX 1.0; ЗАО «ЦБИ-сервис», Россия

20. Сборник тестовых программ Тестовые программы ЗАО «ЦБИ-сервис», Россия

21. Генератор пространственного зашумления Устройство защиты средств вычислительной техники от побочных электромагнитных излучений SEL SP - 21 "Баррикада" (генератор радишума с регулировкой мощности) - на соответствие ТУ и "Сборника норм ... (ПЭМИН)" - для объектов информатизации 2,3 категории SEL SP-21 «Баррикада»; ООО «Сюртель»

22. Генератор пространственного зашумления Генератор шума «ГНОМ-3» - на соответствие «САЗ объектов ЭВТ от утечки информации по побочным излучениям и наводкам. ОТТ» ГНОМ-3; ЗАО «Приборостроитель»

23. Программа инспекционного контроля Проведение инспекционного контроля, пересертификация, контроль целостности и отслеживание изменений версий программных продуктов «ПИК-Эшелон» НПЭШ.00512-01; ЗАО «НПО «Эшелон»

24. Сканер безопасности сетей Программный комплекс «Сканер-ВС» - по 4 уровню контроля отсутствия НДВ и ТУ Сканер-ВС; ЗАО «НПО «Эшелон»

25. Средство анализа исходных текстов Проведение сертификационных испытаний на отсутствие недеklarированных возможностей (программных закладок), анализ безопасности программного кода АК-ВС; ЗАО «НПО «Эшелон»

26. Программное изделие Программное изделие «Поиск USB» предназначено для отображения истории подключений устройств к ПЭВМ по USB-порту и отображения списка недавно сохранённых файлов Поиск USB; ООО «ЦБИ «МАСКОМ», Россия

27. Устройство блокирования средств несанкционированного прослушивания и передачи данных Изделие «КЕДР-1М» предназначено для блокирования работы всех типов устройств несанкционированного прослушивания и передачи данных, аудио- и видео передатчиков, использующих стандарты GSM-900/1800, 3G и 4G, DECT, CDMA, WI-FI и BLUETOOTH КЕДР-1М; ООО «ЦБИ «МАСКОМ», Россия

28. Комплекс противодействия программно-аппаратным воздействиям Комплекс «Рубикон» выполняет функции межсетевого экранирования (МЭ) и системы обнаружения вторжений (СОВ). Предназначен для работы с информацией с грифом до «Совершенно Секретно» Рубикон; ЗАО «НПО «ЭШЕЛОН»

29. Устройство для уничтожения информации Устройство для уничтожения информации, хранящейся на НЖМД СТЕК-НС2.1; НПО «АННА».

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств по дисциплине обеспечивает проверку освоения планируемых результатов обучения (компетенций и их индикаторов) посредством мероприятий текущего, рубежного и промежуточного контроля по дисциплине.

Связь между формируемыми компетенциями и формами контроля их освоения представлена в следующей таблице:

Компетенция	Индикаторы освоения	Аттестационное мероприятие (КП 1)
ПК-2.1	З-ПК-2.1	ЗО, Отч-9
	У-ПК-2.1	ЗО, Отч-9
	В-ПК-2.1	ЗО, Отч-9
ПК-2.2	З-ПК-2.2	ЗО, Отч-9
	У-ПК-2.2	ЗО, Отч-9
	В-ПК-2.2	ЗО, Отч-9
ПК-2.3	З-ПК-2.3	ЗО, Отч-9
	У-ПК-2.3	ЗО, Отч-9
	В-ПК-2.3	ЗО, Отч-9
ПК-2.4	З-ПК-2.4	ЗО, Отч-9
	У-ПК-2.4	ЗО, Отч-9
	В-ПК-2.4	ЗО, Отч-9
УКЦ-1	З-УКЦ-1	ЗО, Отч-9
	У-УКЦ-1	ЗО, Отч-9
	В-УКЦ-1	ЗО, Отч-9
УКЦ-2	З-УКЦ-2	ЗО, Отч-9
	У-УКЦ-2	ЗО, Отч-9
	В-УКЦ-2	ЗО, Отч-9

Шкалы оценки образовательных достижений

Шкала каждого контрольного мероприятия лежит в пределах от 0 до установленного максимального балла включительно. Итоговая аттестация по дисциплине оценивается по 100-балльной шкале и представляет собой сумму баллов, заработанных студентом при выполнении заданий в рамках текущего и промежуточного контроля.

Итоговая оценка выставляется в соответствии со следующей шкалой:

Сумма баллов	Оценка по 4-ех балльной шкале	Оценка ECTS	Требования к уровню освоению учебной дисциплины
90-100	5 – «отлично»	A	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, использует в ответе материал монографической литературы.
85-89	4 – «хорошо»	B	Оценка «хорошо» выставляется студенту, если он твёрдо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.
75-84		C	
70-74		D	
65-69	3 – «удовлетворительно»	E	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные
60-64			

			формулировки, нарушения логической последовательности в изложении программного материала.
Ниже 60	2 – «неудовлетворительно»	F	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

1. 34 И 73 Интеллектуальная защита как базовая составляющая научных исследований : учебное пособие, Саров: РФЯЦ-ВНИИЭФ, 2017
2. 37 К89 Организация научно-исследовательской работы студентов (магистров) : учебное пособие, Москва: ИНФРА-М, 2015
3. 37 Ш51 Научно-исследовательская работа студентов: проблемы и решения : , В. П. Шестак, И. А. Мосичева, Н. В. Скибицкий, Москва: МЭИ, 2006
4. 65 Д64 Справочник по технике безопасности : , П.А. Долин, М.: Энергоатомиздат, 1984

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

1. ЭИ Г 69 Основы теории эксперимента : учебное пособие для вузов, Москва: Юрайт, 2022
2. 001 К63 Планирование и организация научных исследований : учебное пособие (для магистров и аспирантов), Ростов-на-Дону: Феникс, 2014
3. 37 В 75 Труд студента. Ступени успеха на пути к диплому : учебное пособие, Москва: ИНФРА-М, 2019

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

1. СПО «Ревизор -2XP» (Т-211)
2. СПО «Терьер-3.0» (Т-211)
3. СПО «Ревизор сети 1.0» (Т-211)
4. СПО «НКВД» (Т-211)
5. СПО «Агент инвентаризации» (Т-211)

6. СПО «Фикс 2.02» (Т-211)

LMS И ИНТЕРНЕТ-РЕСУРСЫ:

1. Вузовские электронно-библиотечные системы учебной литературы ()

2. База научно-технической информации (например, ВИНТИ РАН) ()

3. www.fstec.ru; www.gost.ru; www.fsb.ru. ()

4. <http://www.scinet.cc> ()

5. <https://bit.spels.ru/index.php/bit> ()

6. <http://library.mephi.ru/> ()

<https://online.mephi.ru/>

<http://library.mephi.ru/>

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

1. специализированная учебная лаборатория: «Контроль защищенности ЛВС от НСД» ()

2. Специализированная учебная лаборатория: «Контроль защищенности ЛВС от НСД» ()

9. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ СТУДЕНТОВ

Преддипломная практика, выполняемая в 4 семестре, направлена на получение оригинальных результатов, имеющих практическую значимость для конкретной организации (предприятия, учреждения) либо имеющих ценность для научно-исследовательских, опытно-конструкторских, учебно-методических работ, выполняемых Аттестационно-испытательным центром информационной безопасности и систем защиты информации, Институтом интеллектуальных кибернетических систем, а также другими структурными подразделениями НИЯУ МИФИ. Работы должны выполняться с учетом и на основании существующей отечественной и международной нормативно-технической базы в рассматриваемой области (стандарты, рекомендации, руководящие документы, законы и подзаконные акты и др.). В работах также должны быть четко и однозначно сформулированы результаты, полученные лично автором, при возможности проведено сравнение с известными образцами, а также указаны инструментальные средства, использовавшиеся в работе. В практической части работ должны быть приведены материалы, свидетельствующие о получении конкретного и четко распознаваемого результата, а также о степени его соответствия действующим нормативно-техническим документам. Материалы являются основой для выполнения ВКР студента.

10. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

Преддипломная практика, выполняемая в 4-м семестре, как правило, направлена на получение аналитических результатов, относящихся к выбранной предметной области, систематизацию, классификацию известных результатов, объектов, моделей или образцов, их

характеристику, параметризацию, сравнение, выявление взаимосвязей между ними, выработку рекомендаций по их практическому применению в различных ситуациях и условиях. Работа, как правило, содержит развернутый аналитический обзор выбранной предметной области, формулировки объекта и предмета исследования, ретроспективу научных и практических результатов в этой области, включая рассмотрение математических и логических основ, формулировки теорем и других доказанных результатов (если имеются), предложения по использованию полученных знаний в последующих работах. Однако следует помнить, что само по себе изучение какого-либо предмета не может являться конечной целью практики – работа должна содержать элементы активного, самостоятельного исследования.

Работа имеет целью преимущественно получение собственных результатов, которые являются итогом решения небольшой по объему и сложности практической либо научно-практической задачи. В такой работе результаты, полученные лично автором, должны быть четко сформулированы и отделены от результатов, заимствованных из других источников. В работе должны быть приведены материалы, свидетельствующие о получении конкретного и четко распознаваемого результата: исходные тексты разработанных программных модулей, экранные формы пользовательских интерфейсов, содержимое файлов настроек и конфигураций, схемы, спецификации, численные результаты расчетов, выведенные математические зависимости и т.п. Темы практики должны быть направлены на получение оригинальных результатов, имеющих практическую значимость для конкретной организации (предприятия, учреждения) либо имеющих ценность для научно-исследовательских, опытно-конструкторских, учебно-методических работ, выполняемых Аттестационно-испытательным центром информационной безопасности и систем защиты информации, Институтом интеллектуальных кибернетических систем, а также другими структурными подразделениями НИЯУ МИФИ. Работы должны выполняться с учетом и на основании существующей отечественной и международной нормативно-технической базы в рассматриваемой области (стандарты, рекомендации, руководящие документы, законы и подзаконные акты и др.). В работах также должны быть четко и однозначно сформулированы результаты, полученные лично автором, при возможности проведено сравнение с известными образцами, а также указаны инструментальные средства, использовавшиеся в работе. В практической части работ должны быть приведены материалы, свидетельствующие о получении конкретного и четко распознаваемого результата, а также о степени его соответствия действующим нормативно-техническим документам. Материалы должны являться основой для выполнения ВКР студента.

Автор(ы):

Дураковский Анатолий Петрович, к.т.н., доцент

Рецензент(ы):

Горбатов В.С.

