Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Национальный исследовательский ядерный университет «МИФИ»

ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ

КАФЕДРА СТРАТЕГИЧЕСКИХ ИНФОРМАЦИОННЫХ ИССЛЕДОВАНИЙ

ОДОБРЕНО УМС ИИКС

Протокол № 8/1/2024

от 28.08.2024 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ПРОИЗВОДСТВЕННАЯ ПРАКТИКА (ПОЛУЧЕНИЕ ПРОФЕССИОНАЛЬНЫХ УМЕНИЙ И ОПЫТА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)

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
5	15	540	540		0	
Итого	15	540	540	0	0	Э

АННОТАЦИЯ

Производственная практика (практика по получению профессиональных умений и опыта профессиональной деятельности, далее ППУ и ОПД) является одной из наиболее важных составных частей процесса подготовки профессионалов в области информационной безопасности в современных условиях.

Производственная практика (ППУ и ОПД) направлена на формирование, закрепление, расширение, углубление и систематизацию знаний, общекультурных, общепрофессиональных, профессиональных компетенций, полученных при изучении теоретических дисциплин в соответствии с видом профессиональной деятельности (информационная безопасность), на которую ориентирована образовательная программа ОБЗОКИИ.

Производственная практика (ППУ и ОПД) является обязательным разделом основной образовательной программы (ООП) магистратуры. Она представляет собой вид учебных занятий, непосредственно ориентированных на получение ППУ и ОПД обучающихся. Результаты производственной практики (ППУ и ОПД) и затем производственной практики (преддипломной) являются продолжением научно-исследовательской работы и в совокупности - основной частью магистерской диссертации, которая в соответствии с программой выполняется в период прохождения практик и выполнения научно-исследовательской работы.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целью производственной практики (ППУ и ОПД) 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 магистранта; 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 обеспечения защиты информации; подготовка магистранта к решению задач комплексного обеспечения информационной безопасности предприятия (объекта защиты), задач, связанных с информационной безопасностью объектов информатизации и к выполнению выпускной квалификационной работы.

Деятельность в период выполнения научно-исследовательской работы обучающихся направлена на формирование универсальных и профессиональных компетенций в соответствии с требованиями ОС ВО НИЯУ МИФИ 10.04.01 и ООП вуза.

В процессе выполнения производственной практики (ППУ и ОПД) студенты должны:

ознакомиться с:

- историей, традициями и организационной структурой подразделения по защите информации;
- организацией систем научно-технического и эксплуатационного обеспечения;
- формами организации производственного процесса и его технологическим обеспечением;
- составом и особенностями эксплуатации технических, программных, аппаратных средств защиты информации;

- используемыми в подразделении методами анализа технологии обработки данных в распределенных системах с целью оптимизации их производительности и повышения надежности функционирования;

- типовыми методами проектирования и оценки эффективности сложных систем в области деятельности подразделения;

- актуальными для подразделения тематиками научных исследований и разработок и оценкой возможности выбора этих тематик в качестве направления или темы для практики и выпускной квалификационной работы.

изучить:

- правила техники безопасности и порядок организации труда на рабочих местах;

- требования режима безопасности и делопроизводства;

- особенности соблюдения специальных правил при работе с оперативно-технической и служебной документацией;

- основные обязанности должностных лиц подразделения по защите информации;

- основные характеристики и возможности, используемых в подразделении технических, программных, аппаратных и криптографических средств защиты информации, методы и тактические приемы их применения для решения задач по обеспечению информационной безопасности объекта;

- общие принципы существующего порядка использования технических и программных средств защиты информации;

- методы применения системного подхода к обеспечению информационной безопасности в различных сферах деятельности подразделения;

- применяемые в подразделении подходы к решению вопросов использования радиоэлектронной аппаратуры и других, технических средств в рамках задач обеспечения информационной безопасности.

закрепить практические навыки:

- проверки, настройки и использования, технических и программных средств подразделения по защите информации;

- выполнения основных функциональных обязанностей в соответствии с должностью;

- работы с технической и эксплуатационной документацией;

- использования современных средств разработки программного обеспечения на языках высокого уровня и языках СУБД, библиотеки объектов и классов для решения задач создания и сопровождения автоматизированных систем;

- реализации системы защиты информации в автоматизированных системах в соответствии со стандартами по оценке защищенных систем.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Производственная практика (ППУ и ОПД)

Образовательные модули, предметы, курсы, дисциплины, на освоении которых базируется научно-исследовательская работа:

Иностранный язык (английский); Методология и организация научных исследований; Защищенные информационные системы; Управление информационной безопасностью; Экономика и управление; Технологии обеспечения информационной безопасности объектов; Целенаправленные атаки на компьютерные системы; Физические основы технических каналов

утечки информации; Основы категорирования значимых объектов критической информационной инфраструктуры.

Требования к «входным» знаниям, умениям и готовностям магистра, приобретенным в результате освоения предшествующих частей образовательной программы и необходимым при освоении программы практики:

знать:

• экономическое планирование и прогнозирование, методику оценки хозяйственной деятельности (применительно к отрасли обеспечения информационной безопасности);

• основные теоретико-числовые методы применительно к задачам защиты информации;

• физические основы функционирования и моделирования, технических средств и систем обработки и передачи информации;

• физические основы образования технических каналов утечки информации;

• методы проведения физического эксперимента при выявлении технических каналов утечки информации;

• основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем;

• методы концептуального проектирования технологий обеспечения информационной безопасности;

владеть:

• самостоятельным построением вероятностных моделей применительно к практическим задачам и проводить статистическую оценку адекватности полученной модели;

• применением систем компьютерной математики для решения типовых задач;

• использованием физических эффектов для обеспечения технической защиты информации;

• применением на практике методов физики при исследовании технических каналов утечки информации;

• осуществлением выбора функциональной структуры системы обеспечения информационной безопасности;

• обоснованием принципов организации технического, программного и информационного обеспечения информационной безопасности;

• организацией работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности;

• навыками управления информационной безопасностью простых объектов.

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
ОПК-3 [1] – Способен разрабатывать проекты организационно-распорядительных документов по обеспечению	З-ОПК-3 [1] – Знать: основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, в области управления информационной безопасностью

информационной безопасности	У-ОПК-3 [1] – Уметь: проводить выбор, исследовать эффективность, проводить технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности; разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации В-ОПК-3 [1] – Владеть: навыками разработки политик безопасности различных уровней и работы с нормативными правовыми актами в области информационной безопасности
ОПК-4 [1] – Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок	З-ОПК-4 [1] – Знать: способы формулирования научной проблемы, гипотезы, выбора предмета, объекта, целей, задач исследования; методы анализа и обоснования выбора решений по обеспечению требуемого уровня безопасности информационных систем У-ОПК-4 [1] – Уметь: разрабатывать планы и программы проведения научных исследований в соответствии с техническим заданием, ресурсным обеспечением и заданными сроками выполнения работы В-ОПК-4 [1] – Владеть: навыками структурирования информации по теме исследования и самостоятельного научного мышления, обобщения и систематизации информации
ОПК-5 [1] – Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи	З-ОПК-5 [1] – Знать: теоретические и эмпирические методы научных исследований, порядок проведения научных исследований У-ОПК-5 [1] – Уметь: применять методы научных исследований в научной деятельности, обобщать полученные экспериментальные данные, анализировать и делать выводы В-ОПК-5 [1] – Владеть: теоретическими и эмпирическими методами научного исследования при выполнении научно-исследовательских работ, методикой оформления отчетов по научно-исследовательским работам, статей и тезисов докладов

Профессиональные компетенции в соотвествии 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**
контрольно-аналитический			
Контроль защищенности ЗО	Объекты информатизации,	ПК-4 [1] - Способен участвовать в	З-ПК-4[1] - Знать: методы и методики

КИИ по требованиям безопасности информации; аттестация ЗО КИИ по требованиям безопасности информации; проведение сертификационных испытаний средств защиты информации ЗО КИИ на соответствие требованиям по безопасности информации	информационные ресурсы и информационные технологии, компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы, обеспечивающие безопасность критических процессов значимых объектов критической информационной инфраструктуры	планировании и реализации процессов контроля ИБ или процессов информационно-аналитических систем безопасности *Основание:* Профессиональный стандарт: 06.032, 06.034	оценки безопасности программно-аппаратных средств защиты информации; принципы построения программно-аппаратных средств защиты информации; принципы построения подсистем защиты информации в компьютерных системах; методы и методики контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок; средства контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок; средства контроля защищенности информации от несанкционированного доступа порядок аттестации объектов информатизации на соответствие требованиям по защите информации; способы организации работ при проведении сертификации программно-аппаратных средств защиты; нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и сертификации средств защиты информации на соответствие

			требованиям по безопасности информации. ; У-ПК-4[1] - Уметь: оценивать эффективность защиты информации; применять разработанные методики оценки защищенности программно-аппаратных средств защиты информации; оформлять материалы аттестационных испытаний (протоколов аттестационных испытаний и заключения по результатам аттестации объектов вычислительной техники на соответствие требованиям по защите информации); анализировать компьютерную систему с целью определения уровня защищенности и доверия; применять инструментальные средства проведения сертификационных испытаний; разрабатывать программы и методики сертификационных испытаний программных (программно-технических) средств защиты информации от несанкционированного доступа на соответствие требованиям по безопасности

			информации; проводить экспертизу технических и эксплуатационных документов на сертифицируемые программные (программно-технические) средства защиты информации от несанкционированного доступа и материалов сертификационных испытаний. ; В-ПК-4[1] - Владеть: определением уровня защищенности и доверия программно-аппаратных средств защиты информации; основами проведения аттестационных испытаний объектов вычислительной техники на соответствие требованиям по защите информации; основами проведения экспериментальных исследований уровней защищенности компьютерных систем и сетей; основами подготовки протоколов испытаний и технического заключения по результатам сертификационных испытаний программных (программно-технических) средств защиты информации от несанкционированного доступа на соответствие требованиям по безопасности

			информации; основами проведения экспертизы технических и эксплуатационных документов на сертифицируемые программные (программно-технические) средства защиты информации от несанкционированного доступа и материалов сертификационных испытаний.
педагогический			
Выполнение учебной и методической работы в образовательных организациях среднего профессионального образования, высшего образования и дополнительного профессионального образования (ДПО) по дополнительным профессиональным программам (ДПП) в должностях преподавателя и ассистента по дисциплинам направления	Методы и средства проектирования, моделирования и экспериментальной отработки систем, средств и технологий обеспечения информационной безопасности значимых объектов критической информационной инфраструктуры; Образовательный процесс в области обеспечения безопасности значимых объектов критической информационной инфраструктуры.	ПК-5 [1] - Способен руководить научно-исследовательской деятельностью обучающихся по программе бакалавриата (направление информационная безопасность) *Основание:* Профессиональный стандарт: 01.002	З-ПК-5[1] - Знать: методологию научного исследования, особенности научного исследования в соответствующей отрасли знаний и (или) методология проектной деятельности, особенности проектной деятельности в соответствующей области; теоретические основы и технология научно-исследовательской и проектной деятельности ; У-ПК-5[1] - Уметь: применять нормативные правовые акты и методические документы на всех этапах подготовки и оформления проектных, исследовательских, выпускных квалификационных работ, прохождения практики. ; В-ПК-5[1] - Владеть: методиками

			оформления методики проектных, исследовательских работ обучающихся по программам во и (или) дпп, в том числе выпускных квалификационных работ (если их выполнение предусмотрено реализуемой образовательной программой); организацией подготовки и проведения научных конференций, конкурсов; проектных и исследовательских работ обучающихся .

4. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

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

№ п.п	Наименование раздела учебной дисциплины	Недели	Лекции/ Практ. (семинары)/ Лабораторные работы, час.	Обязат. текущий контроль (форма*, неделя)	Максимальный балл за раздел**	Аттестация раздела (форма*, неделя)	Индикаторы освоения компетенции
	5 Семестр						
1	Получение задания, подготовка отчёта, защита практики	1-10	0/540/0		50	Отч-15	З-ОПК-3, У-ОПК-3, В-ОПК-3, З-ОПК-4, У-ОПК-4, В-ОПК-4, З-ОПК-5, У-ОПК-5, В-ОПК-5, З-ПК-4, У-ПК-4, В-ПК-4, З-ПК-5, У-ПК-5, В-ПК-5
	Итого за 5 Семестр		0/540/0		50		
	Контрольные мероприятия за 5				50	Э	З-ОПК-3, У-ОПК-3,

	Семестр						В-ОПК-3, З-ОПК-4, У-ОПК-4, В-ОПК-4, З-ОПК-5, У-ОПК-5, В-ОПК-5, З-ПК-4, У-ПК-4, В-ПК-4, З-ПК-5, У-ПК-5, В-ПК-5

* – 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

Недели	**Темы занятий / Содержание**	**Лек., час.**	**Пр./сем., час.**	**Лаб., час.**
	5 Семестр	0	540	0
1-10	**Получение задания, подготовка отчёта, защита практики**	0	540	0
1 - 7	**Постановка задачи и выполнение работы** Согласование с руководителем и консультантом задания на практику. Инструктаж по технике безопасности на рабочем месте. Выполнения практического задания по месту прохождения практики.	Всего аудиторных часов		
		0	252	0
		Онлайн		
		0	0	0
8 - 14	**Выполнение работы** Выполнения практического задания по месту прохождения практики.	Всего аудиторных часов		
		0	252	0
		Онлайн		
		0	0	0
15	**Подготовка отчета, защита практики** Оформление отчёта о практике. Подготовка доклада и презентации. Защита практики.	Всего аудиторных часов		
		0	36	0
		Онлайн		
		0	0	0

Сокращенные наименования онлайн опций:

Обозначение	**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

ТЕМЫ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Недели	**Темы занятий / Содержание**
	5 Семестр
1 - 7	**Постановка задачи и выполнение работы** Согласование с руководителем и консультантом задания на практику. Инструктаж по технике безопасности на рабочем месте. Выполнения практического задания по месту прохождения практики.
8 - 14	**Выполнение работы** Выполнения практического задания по месту прохождения практики.
15	**Подготовка отчета, защита практики** Оформление отчёта о практике. Подготовка доклада и презентации. Защита практики.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Цель прохождения практики (ППУ И ОПД) 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.

При реализации практики ППУ и ОПД используются различные образовательные технологии – во время аудиторных занятий занятия проводятся в форме практических занятий.

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 дискоконусная антенна DA-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, обрабат-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 обектов 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 XP; ЗАО «ЦБИ-сервис», Россия

16. Анализатор уязвимостей СЗИ СВТ от НСД Программа для анализа уязвимостей средств защиты СВТ от НСД Ревизор-2 XP; 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 радиошума 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 недекларированных 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)**
ОПК-3	З-ОПК-3	ЗО, Отч-15
	У-ОПК-3	ЗО, Отч-15
	В-ОПК-3	ЗО, Отч-15
ОПК-4	З-ОПК-4	ЗО, Отч-15
	У-ОПК-4	ЗО, Отч-15
	В-ОПК-4	ЗО, Отч-15
ОПК-5	З-ОПК-5	ЗО, Отч-15
	У-ОПК-5	ЗО, Отч-15
	В-ОПК-5	ЗО, Отч-15

ПК-4	З-ПК-4	ЗО, Отч-15
	У-ПК-4	ЗО, Отч-15
	В-ПК-4	ЗО, Отч-15
ПК-5	З-ПК-5	ЗО, Отч-15
	У-ПК-5	ЗО, Отч-15
	В-ПК-5	ЗО, Отч-15

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*»		Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала.
60-64		E	
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, Николаева В.Е. [и др.], Саров: РФЯЦ-ВНИИЭФ, 2017

2. ЭИ П 18 Методы и модели исследования сложных систем и обработки больших данных : монография, Хомоненко А. Д. [и др.], Санкт-Петербург: Лань, 2020

3. 37 Ш51 Научно-исследовательская работа студентов: проблемы и решения : , Скибицкий Н.В., Шестак В.П., Мосичева И.А., Москва: МЭИ, 2006

4. 37 К89 Организация научно-исследовательской работы студентов (магистров) : учебное пособие, Кукушкина В.В., Москва: ИНФРА-М, 2015

5. 001 К63 Планирование и организация научных исследований : учебное пособие (для магистров и аспирантов), Комлацкий В.И., Комлацкий Г.В., Логинов С.В., Ростов-на-Дону: Феникс, 2014

6. 65 Д64 Справочник по технике безопасности : , Долин П.А., М.: Энергоатомиздат, 1984

7. 37 В 75 Труд студента. Ступени успеха на пути к диплому : учебное пособие, Воронцов Г. А., Москва: ИНФРА-М, 2019

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

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, ВИНИТИ 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

Производственная практика (ППУ и ОПД), выполняемая в 5 семестре, направлена на получение оригинальных результатов, имеющих практическую значимость для 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 либо конкретной организации (предприятия, учреждения). 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 преддипломной практики и написания ВКР студента, 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 преддипломной практики и написания ВКР студента.

10. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

Производственная практика (ППУ и ОПД), выполняемая в 5 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 преддипломной практики и написания ВКР студента.

Автор(ы):

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

Рецензент(ы):
Горбатов