МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»

УТВЕРЖДАЮ:
Директор института
Энергетики и автоматизированных систем
_____ С.И. Лукьянов
«15» марта 2017 г.

ПРОГРАММА ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ ПО ПОЛУЧЕНИЮ ПРОФЕССИОНАЛЬНЫХ УМЕНИЙ И ОПЫТА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Специальность
10.05.03 Информационная безопасность автоматизированных систем
шифр наименование специальности

Специализация программы
Обеспечение информационной безопасности распределенных информационных систем
наименование специализации

Уровень высшего образования
специалитет

Форма обучения
очная

Институт	Энергетики и автоматизированных систем
Кафедра	Информатики и информационной безопасности
Курс	4
Семестр	8

Магнитогорск
2017 г.

Рабочая программа составлена на основе ФГОС ВО по специальности 10.05.03 «Информационная безопасность автоматизированных систем», утвержденного приказом МОиН РФ от 01.12.2016 № 1509.

Рабочая программа рассмотрена и одобрена на заседании кафедры
Информатики и информационной безопасности
(наименование кафедры - разработчика)

«03» марта 2017 г., протокол № 10.

Зав. кафедрой _____ /И.И. Баранкова/
(подпись) (И.О. Фамилия)

Рабочая программа одобрена методической комиссией
института Энергетики и автоматизированных систем
(наименование факультета (института) - исполнителя)

«14» марта 2017 г., протокол № 6.

Председатель _____ / С.И. Лукьянов/
(подпись) (И.О. Фамилия)

Рабочая программа составлена: зав.кафедрой ИиИБ, д.т.н., профессор
(должность, ученая степень, ученое звание)

_____ / И.И. Баранкова /
(подпись) (И.О. Фамилия)

Рецензент: зав. кафедрой Бизнес-информатики
и информационных технологий, к.п.н. профессор
(должность, ученая степень, ученое звание)

_____ / Г.Н. Чусавитина/
(подпись) (И.О. Фамилия)

Лист регистрации изменений и дополнений

№ п/п	Раздел программы	Краткое содержание изменения/дополнения	Дата, № протокола заседания кафедры	Подпись зав. кафедрой
1.	7	Переработка фонда оценочных средств	№1 от 20.09.2017	
2.	8	Обновление списка основной и дополнительной литературы	№1 от 20.09.2017	
3.	7	Переработка фонда оценочных средств	№1 от 07.09.2018	
4.	8	Обновление списка основной и дополнительной литературы	№1 от 07.09.2018	
5.	7	Переработка фонда оценочных средств	№ 1 от 07.09.2019	
6.	8	Обновление списка основной и дополнительной литературы	№ 1 от 07.09.2019	
7.	7	Переработка фонда оценочных средств	№1 от 04.09.2020	
8.	8	Обновление списка основной и дополнительной литературы	№1 от 04.09.2020	

1 Цели практики

Целями производственной практики по получению профессиональных умений и опыта профессиональной деятельности для специальности 10.05.03 «Информационная безопасность автоматизированных систем» являются: закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование 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.

2 Задачи практики

Задачами производственной практики по получению профессиональных умений и опыта профессиональной деятельности являются закрепление, расширение, углубление и систематизацию знаний, полученных при изучении общепрофессиональных и специальных дисциплин, на основе изучения деятельности конкретной организации, приобретение первоначального практического опыта.

Программа практики по специальности обеспечивает обоснованную последовательность формирования у студентов единой системы профессиональных умений и навыков в соответствии с профилем деятельности специалиста. При организации и проведении практики заложен модульный принцип, который осуществляет привязку задания к конкретному предприятию, обеспечивающему его выполнение.

3 Место практики в структуре образовательной программы

Для прохождения практики необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:

Организация ЭВМ и вычислительных систем

Информатика

Языки программирования

Сети и системы передачи информации

Учебная-практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности

Основы информационной безопасности

Технология построения защищенных распределенных приложений

Программно-аппаратные средства обеспечения информационной безопасности

Безопасность сетей ЭВМ

Безопасность систем баз данных

Техническая защита информации

Методы выявления нарушений информационной безопасности, аттестация АИС

Организационное и правовое обеспечение информационной безопасности

Информационная безопасность распределенных информационных систем

Безопасность операционных систем

Разработка и эксплуатация защищенных автоматизированных систем

Методы мониторинга информационной безопасности АС

Криптографические методы защиты информации

Знания (умения, владения), полученные в процессе прохождения практики будут необходимы для изучения дисциплин/практик:

Анализ рисков информационной безопасности

Виртуальные сети
Защита программного обеспечения
Информационная безопасность систем организационного управления
Моделирование систем и процессов защиты информации
Научно-исследовательская работа
Производственная-преддипломная практика
Подготовка к сдаче и сдача государственного экзамена
Подготовка к защите и защита выпускной квалификационной работы

4 Место проведения практики

Производственная практика по получению профессиональных умений и опыта профессиональной деятельности проводится на базе кафедры «Информатики и информационной безопасности», в лабораториях технических средств защиты информации, защищенных автоматизированных систем, программно-аппаратных средств обеспечения информационной безопасности, сетей и систем передачи информации, безопасности сетей ЭВМ ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова», ООО «ММК-Информсервис», ПАО «Магнитогорский металлургический комбинат», и других предприятиях г. Магнитогорска, а также Управление ФСТЭК России по УрФО, г. Екатеринбург.

Способ проведения практики: выездная и/или стационарная

Практика осуществляется дискретно

5 Компетенции обучающегося, формируемые в результате прохождения практики и планируемые результаты обучения

В результате прохождения практики обучающийся должен обладать следующими компетенциями:

Структурный элемент компетенции	Планируемые результаты обучения
ПСК-7.1 способностью разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах	
Знать	- нормативные правовые акты в области защиты информации; - национальные, межгосударственные и международные стандарты в области защиты информации; - руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации. - порядок разработки модели угроз - виды нарушителей информационной безопасности
Уметь	- оценивать информационные риски в автоматизированных системах; - классифицировать и оценивать угрозы безопасности информации; - определять подлежащие защите информационные ресурсы автоматизированных систем; - анализировать изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации - оценивать потенциал нарушителя информационной безопасности - применять базовую модель угроз ПДн

Владеть	- методами выявления угроз безопасности информации в автоматизированных системах; - методами оценки последствий от реализации угроз безопасности информации в автоматизированной системе. - навыками применения базовой модели угроз ПДн
ПСК-7.2 способностью проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах	
Знать	- Порядок разработки политик безопасности; - методы и процедуры выявления угроз информационной безопасности в защищённых распределённых системах;
Уметь	- оценивать информационные риски в автоматизированных системах; - выполнять анализ рисков информационной безопасности в распределенных информационных системах; - анализировать и оценивать угрозы информационной безопасности объекта, выполнять анализ рисков информационной безопасности в распределенных информационных системах. - определить перечень необходимых политик безопасности
Владеть	- методиками проведения анализа рисков информационной безопасности распределенных информационных систем; - методами оценки информационных рисков; - навыками разработки политики информационной безопасности автоматизированных систем.
ПСК-7.3 способностью проводить аудит защищенности информационно- технологических ресурсов распределенных информационных систем	
Знать	─ Источники и классификацию угроз информационной безопасности; ─ Основные принципы построения систем защиты информации; ─ Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации. ─ Методы и порядок проведения аудита защищенности информационно- технологических ресурсов
Уметь	─ Выявлять уязвимости информационно-технологических ресурсов автоматизированных систем; ─ Участвовать в проведении мониторинга угроз безопасности автоматизированных систем; ─ Самостоятельно проводить мониторинг угроз безопасности автоматизированных систем; ─ Проводить аудит защищенности информационно- технологических ресурсов
Владеть	─ Методами выявления угроз информационной безопасности автоматизированных систем; ─ Методами аудита уровня защищенности АИС.
ПСК-7.4 способностью проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах	

Знать	- принципы построения и функционирования, архитектуру, примеры реализаций современных систем управления базами данных; - основные модели данных, физическую организацию баз данных; - последовательность и содержание этапов проектирования баз данных; - основные средства и методы удаленного администрирования операционных систем и систем баз данных в распределенных информационных системах
Уметь	- разрабатывать и администрировать базы данных в соответствии с требования информационной безопасности; -настраивать защиту программного обеспечения с применением дистанционного администрирования -настраивать удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах
Владеть	- методами настройки безопасной работы с БД с помощью современных образцов программных, технических средств; -в полной мере средствами администрирования БД в интегрированных средах СУБД. -средствами удаленного администрирования операционных систем и систем баз данных в распределенных информационных системах -навыками удаленного администрирования операционных систем и систем баз данных в распределенных информационных системах
ПСК-7.5 способностью координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении	
Знать	-основные методы организации обеспечения информационной безопасности; - принципы организации обеспечения информационной безопасности - организационные меры защиты информации
Уметь	-анализировать эффективность систем защиты информации и разрабатывать направления ее развития; -организовывать и обеспечивать сохранение режима государственной тайны; - организовывать и обеспечивать сохранение режима конфиденциальности; -формировать требования к защите информации, содержащейся в информационной системе -определить цели и задач защиты информации в информационной системе, основные этапы создания системы защиты информации
Владеть	-методами формирования требований по защите объекта; -навыками разработки организационно-распорядительных документов
ОПК-3 способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности	
Знать	-Общие принципы построения современных языков программирования высокого уровня. -Язык программирования высокого уровня (объектно-ориентированное программирование).

Уметь	-Работать с интегрированной средой разработки программного обеспечения. -Использовать шаблоны классов и средства макрообработки. -Использовать динамически подключаемые библиотеки. -Проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения.
Владеть	-Навыками реализации основных структур данных и базовых алгоритмов средствами языков программирования. -Навыками работы с интегрированной средой разработки программного обеспечения.
ОПК-6 способностью применять нормативные правовые акты в профессиональной деятельности	
Знать	-основы организационного и правового обеспечения информационной безопасности, -основные нормативные правовые акты в области обеспечения информационной безопасности - нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации;
Уметь	-применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности
Владеть	-навыками работы с нормативными правовыми актами
ОПК-8 способностью к освоению новых образцов программных, технических средств и информационных технологий	
Знать	-Классификацию современных программных и программноаппаратных СЗИ. -Состав, назначение функциональных компонентов и программного обеспечения программных и программно-аппаратных средств ЗИ. -Типовые структуры и принципы организации программных и программно-аппаратных СЗИ.
Уметь	-Осуществлять сбор, обработку, анализ и систематизацию научно-технической информации в области программных и программно-аппаратных средств ЗИ и систем с применением современных информационных технологий. -Основные принципы работы всех подсистем системы ИБ АС.
Владеть	- Навыками работы с подсистемами системы информационной безопасности автоматизированной системы. - Навыками администрирования системы ИБ АС.
ПК-3 способностью проводить анализ защищенности автоматизированных систем	
Знать	- Критерии оценки эффективности и надежности средств защиты распределенных информационных систем - Принципы построения и функционирования распределенных информационных систем в защищённом исполнении -Мероприятия для обеспечения защиты информации

Уметь	-Анализировать техническую и сопроводительную документацию по обеспечению ИБ. -Анализировать целесообразность выбора технических, программно–аппаратных и криптографических компонентов автоматизированных систем с целью совершенствования защиты. -Проводить контроль за событиями безопасности и действиями пользователей в информационной системе -Проводить анализ и оценку функционирования системы защиты информации информационной системы
Владеть	-Навыками выбора средств защиты информации -Навыками документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе
ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	
Знать	-Базовую модель угроз ПДн -Нормативно-методические документы в области моделирования угроз -Способы реализации угроз безопасности информации -Типы нарушителя информационной безопасности в автоматизированных системах -Методику разработки модели угроз
Уметь	-Разрабатывать частную модель угроз автоматизированной системы -Определять актуальные угрозы для автоматизированной системы; -Разрабатывать модель нарушителя информационной безопасности автоматизированных систем информационно-технологических ресурсов автоматизированных систем.
Владеть	- Навыками определения информационной инфраструктуры и информационных ресурсов организации, подлежащих защите; - Навыками разработки частных моделей угроз
ПК-5 способностью проводить анализ рисков информационной безопасности автоматизированной системы	
Знать	- методологию анализа рисков информационной безопасности; - методики определения информационно-технологических ресурсов, подлежащих защите;
Уметь	- выполнять анализ особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите. -оценить риски информационной безопасности автоматизированной системы
Владеть	- навыками анализа рисков информационной безопасности автоматизированных систем -методиками анализа рисков
ПК-6 способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности	

Знать	─ источники и классификацию угроз информационной безопасности; ─ основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; ─ основные угрозы безопасности информации и модели нарушителя в автоматизированных системах;
Уметь	─ анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем; ─ классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; ─определять параметры настройки программного обеспечения, включая программное обеспечение средств защиты информации, состава и конфигурации технических средств и программного обеспечения поддерживать конфигурацию информационной системы и ее системы защиты информации
Владеть	─ навыками документирования действий по внесению изменений в базовую конфигурацию информационной системы и ее системы защиты информации ─ методами формирования требований по защите информации; ─ навыками анализа основных узлов и устройств современных автоматизированных систем; ─ навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем ─ навыками обеспечения защиты информации при выводе из эксплуатации аттестованной информационной системы
ПК-7 способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ	
Знать	-нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности, структуру научно-технических отчетов
Уметь	-принимать участие в разработке проектов нормативных и организационно- распорядительных документов, регламентирующих работу по защите информации; - применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности
Владеть	-навыками разработки научно-техническую документации, научно-технических отчетов по результатом выполненных работ
ПК-8 способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем	
Знать	─ методы разработки и анализа проектных решения по обеспечению безопасности автоматизированных систем; ─ современную нормативно-правовую базу создания защищенных распределенных информационных систем; ─ инструментальные программные и аппаратные средства анализа защищенности информационных систем и сетей

Уметь	─ разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем; ─ применять современные аппаратные средства защиты информационных процессов при аудите распределенных компьютерных систем
Владеть	─ методиками разработки и анализа проектных решения по обеспечению безопасности автоматизированных систем; ─ навыками разработки комплексной инфраструктуры защищенной информационной системы; ─ навыками работы с ведущими программными и аппаратными комплексными средствами защиты информации
ПК-9 способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности	
Знать	- Понятия функциональной и системной архитектуры информационных систем, ядра безопасности информационных систем - Основные принципы построения защищенных распределенных компьютерных систем - Документы ФСТЭК России, регламентирующие порядок разработки моделей угроз в автоматизированных системах. - Современные принципы построения архитектуры ИС.
Уметь	- Осуществлять анализ несложных процессов проектирования; - Применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования средств защиты информации компьютерной системы - разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов
Владеть	- Способами определения уровней защищенности и доверия программно-аппаратных средств защиты информации - Практическими навыками определения уровня защищенности и доверия программно-аппаратных средств защиты информации - Определять уровни защищенности и доверия программно-аппаратных средств защиты информации • Приемами разработки моделей автоматизированных систем и подсистем безопасности автоматизированных систем - Приемами разработки проектов нормативных документов, регламентирующих работу по защите информации - Навыками разработки технических заданий на создание подсистем информационной безопасности автоматизированных систем; - Навыками разработки предложений по совершенствованию системы управления безопасностью информации в автоматизированных системах
ПК-10 способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности	

Знать	- Современные технологии программирования. - Основные виды интегрированных сред разработки программного обеспечения. - Современные технологии и методы программирования, предназначенные для создания прикладных программ в защищенном исполнении. - Принципы работы элементов и функциональных узлов электронной аппаратуры; -Типовые схемотехнические решения основных узлов и блоков электронной аппаратуры - Принципы функционирования и основные рабочие характеристики оборудования сетей ЭВМ;
Уметь	- Реализовывать на языке высокого уровня алгоритмы решения профессиональных задач; - Работать с основными средами интегрированной разработки программного обеспечения; - Проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения; - Реализовывать разработанную структуру классов для задач предметной области. -Работать с современной элементной базой электронной аппаратуры; -Использовать стандартные методы и средства проектирования цифровых узлов и устройств, в том числе для средств защиты информации - Разрабатывать топологию вычислительной сети в соответствии с требованиями технического задания.
Владеть	- Навыками реализации алгоритмов на языках программирования высокого уровня; - Навыками пользования библиотеками прикладных программ для решения прикладных задач профессиональной области. - Способностью использовать языки, системы и инструментальные средства разработки автоматизированных систем. -Навыками чтения принципиальных схем, построения временных диаграмм и восстановления алгоритма работы узла, устройства и системы по комплексу документации; - Методиками проектирования топологии вычислительных сетей; - Навыками настройки сетевого оборудования.
ПК-11 способностью разрабатывать политику информационной безопасности автоматизированной системы	
Знать	- систему организационных мер, направленных на защиту информации ограниченного доступа - нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа; - уровни политик информационной безопасности назначение политик верхнего, среднего и нижнего уровня

Уметь	- разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации; -разрабатывать политики, относящиеся к определенным аспектам использования информационных технологий, организации информационных потоков и организации работы персонала
Владеть	- владеть навыками разработки политик безопасности различных уровней. -владеть навыками формирования комплекта организационной документации, относящихся к обеспечению безопасности отдельных элементов информационных систем, информационных потоков и массивов информации
ПК-12 способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы	
Знать	- особенности решений по ЗИ в информационных процессах и системах; - определения рисков ИБ применительно к ОИ с заданными характеристиками; - методы и подходы к реализации системы управления безопасностью АИС; - методы анализа процессов для определения актуальных угроз
Уметь	- оценивать различные инструменты в области проектирования и управления ИБ; - разрабатывать политики безопасности информации АС; - разрабатывать нормативно-методические материалы по регламентации системы организационной ЗИ.
Владеть	- навыками управления рисками ИБ, навыками разработки положения о применимости механизмов контроля в контексте управления рисками ИБ.
ПК-13 способностью участвовать в проектировании средств защиты информации автоматизированной системы	
Знать	- способы организации обмена данными при помощи технологий RPC,RMC и очередей; - криптографические протоколы обмена информацией; - общий порядок действий по выбору мер защиты информации для их реализации в информационной системе - методы проектирования средств защиты информации;
Уметь	- разрабатывать программное обеспечение по технологии Socket с учетом возможных состояний передающей, приемной сторон и линии связи; - разрабатывать и исследовать модели информационно-технологических ресурсов, проектировать средства защиты информации АС - выбрать меры защиты информации для их реализации в информационной системе в рамках ее системы защиты информации
Владеть	- навыками оформления программной документации по ЕСПД; - методами исследования информационно-технологических ресурсов -навыками определения необходимого набора мер защиты информации (базового, адаптированного, уточненного)

ПК-14 способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	
Знать	- Способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации. - Способы контрольных проверок работоспособности и эффективности применяемых технических средств защиты информации. - Способы контрольных проверок работоспособности и эффективности применяемых программных и программно- аппаратных СЗИ.
Уметь	- Участвовать в настройке технических средств обеспечения информационной безопасности. - Самостоятельно настраивать технические средства обеспечения информационной безопасности. - Исследовать эффективность контрольных проверок работоспособности применяемых технических средств защиты информации. - Применять технические средства обеспечения информационной безопасности. - Исследовать эффективность контрольных проверок работоспособности применяемых программных и программно-аппаратных СЗИ. - Применять программные и программно-аппаратные средства обеспечения ИБ.
Владеть	- Техникой настройки технических средств обеспечения информационной безопасности - Навыками использования технических средств обеспечения информационной безопасности автоматизированных систем. - Навыками анализа архитектурно-технических и схемотехнических решений компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем. - Навыками использования программных и программно-аппаратных средств обеспечения ИБ АС.
ПК-15 способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем	
Знать	-уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий; - положение о системе сертификации средств защиты информации; -продукцию, которую необходимо сертифицировать; -состав участников системы сертификации и их основные функции; -этапы сертификации; - требования к проведению испытаний СЗИ; -порядок проведения сертификационных испытаний

Уметь	─ составлять заявку на сертификацию средств защиты информации/продление срока действия сертификата соответствия; ─ проводить анализ решения о проведении сертификации средства защиты информации /сертификационных испытаний для продления срока действия сертификата соответствия ─ проводить анализ сертификата соответствия.
Владеть	─ нормативно-правовой базой в области сертификации средств защиты информации ─навыками проведения испытаний средств защиты информации,
ПК-16 способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации	
Знать	─ Средства анализа информационной безопасности; ─ Классификацию систем защиты информации; ─ Средства организации аттестации по требованиям безопасности информации
Уметь	─ Принимать участие в аттестационных испытаниях системы защиты информации и анализе результатов; ─ Проводить научно-исследовательские работы при аттестации системы защиты информации с учетом требований по обеспечению информационной безопасности.
Владеть	─ Навыками использования средств анализа информационной безопасности; ─ Навыками проведения аттестации в соответствии с существующими нормативами.
ПК-17 способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	
Знать	- перечень инструментов для проведения мониторинга защищенности информации; - базовый функционал инструментов для проведения мониторинга защищенности информации;
Уметь	- применять технические средства для проведения мониторинга беспроводных сетей; - применять технические средства для проведения мониторинга проводных сетей построенных на основе неуправляемых коммутаторов;
Владеть	- навыками работы с специализированным программным обеспечением для проведения мониторинга защищенности информации в автоматизированной системе;
ПК-18 способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности	
Знать	-организацию деятельности службы безопасности объекта по основным направлениям работ по защите информации -организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации;

Уметь	-применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности -анализировать и обобщения информации на стадии принятия и реализации управленческого решения, -пользоваться конструктивной критикой, учитывать мнения коллег и подчиненных, осуществлять подбор и расстановки кадров
Владеть	-навыками ведения деловых переговоров, публичного выступления, взаимодействия с другими ведомствами, государственными органами, представителями субъектов Российской Федерации, муниципальных образований, -методами организации и управления деятельностью служб защиты информации на предприятии -навыками организации и обеспечения режима секретности -навыками планирования работы, контроля, анализа и прогнозирования последствий принимаемых решений, стимулирования достижения результатов
ПК-19 способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы	
Знать	- нормативные методические документы ФСТЭК России в области ИБ; - основные принципы создания системы управления информационной безопасностью. - методы реализации системы управления безопасностью
Уметь	- проводить оценку информационных рисков, - обосновывать решения по обеспечению ИБ объектов в профессиональной сфере деятельности; - расследовать инциденты ИБ; - разрабатывать предложения по совершенствованию СУИБ АС.
Владеть	- навыками расчета и управления рисками ИБ; - навыками разработки положения о применимости механизмов контроля в контексте управления рисками ИБ. - навыками подготовки документации СУИБ
ПК-20 способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности	
Знать	- Основы организационного и правового обеспечения ИБ. - Основные нормативные и правовые акты в области обеспечения ИБ. - Нормативные методические документы ФСБ РФ и ФСТЭК РФ в области ЗИ. - классификацию информационных систем по требованиям защиты информации.

Уметь	- Определять класс защищенности информационной системы - Принимать участие в реализации разработанной АС с учетом требований информационной безопасности. - Готовить сопроводительную документацию к разработанной АС в защищенном исполнении. - Осуществлять контроль эффективности применения разработанной АС в защищенном исполнении. - выбирать меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы - определять виды и типы средств защиты информации, обеспечивающие реализацию технических мер защиты информации
Владеть	- Навыками разработки автоматизированных систему с учетом требований ИБ. - Навыками контроля разработки АС с учетом требований ИБ. - Навыками выбора средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации - Навыками разработки сопроводительной документации к разработанной подсистеме защиты информации АС
ПК-21 способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	
Знать	─ нормативные требования по защите информации; критерии оценки защищенности АС; способы анализа и оценке угроз информационной безопасности; ─ организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации;
Уметь	─ применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; ─ разрабатывать, реализовывать, оценивать и корректировать процессы менеджмента информационной безопасности; ─ разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем
Владеть	─ навыками администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности; ─ нормативными требованиями по защите информации; ─ навыками организации и обеспечения режима секретности ─ навыками разработки организационно-распорядительных документов
ПК-22 способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	

Знать	- основные угрозы безопасности информации и модели нарушителя ОИ; - принципы формирования политики информационной безопасности организации. - способы контроля эффективности реализации политики информационной безопаности
Уметь	- разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих ЗИ ограниченного доступа в организации; - разрабатывать нормативно-методические материалы по регламентации системы организационной ЗИ; - разрабатывать частные политики ИБ АС; - контролировать эффективность принятых мер по реализации частных политик ИБ АС.
Владеть	- навыками разработки политик безопасности различных уровней. - навыками и методами контроля эффективности сформированной политики информационной безопасности
ПК-23 способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	
Знать	- Методы формирования требований по защите информации ограниченного доступа - Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации ограниченного доступа - Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем. - Организационные меры по защите информации ограниченного доступа
Уметь	- Использовать методы формирования требований по защите информации ограниченного доступа - Классифицировать средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации ограниченного доступа
Владеть	- Методами формирования требований по защите информации ограниченного доступа - Навыками анализа методов формирования требований по защите информации ограниченного доступа
ПК-24 способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	
Знать	- методы повышения уровня безопасности за счет настройки прав доступа к ресурсам автоматизированной системы;
Уметь	- применять меры организационного и программно-технического уровня, направленных на защиту информационно-технологических ресурсов автоматизированной системы - выявлять узлы автоматизированной системы, не обеспечивающие требуемый уровень защиты информации
Владеть	- навыками определения возможных векторов атаки на автоматизированную систему и осуществлять выбор средств защиты информации;

ПК-25 способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций	
Знать	- Принципы администрирования баз данных. Средства обеспечения безопасности данных. - Организацию защиты информации баз данных. Сравнительный анализ эффективности применения средств обеспечения безопасности данных
Уметь	- Анализировать работоспособность базы данных. - Принимать участие в настройке средств обеспечения безопасности данных, обрабатываемых в СУБД. - Самостоятельно применять средства обеспечения безопасности данных. - Участвовать в восстановлении работоспособности систем баз данных при возникновении нештатных ситуаций. - Организовывать безопасность систем баз данных - Выявлять инциденты и реагировать на них - Устанавливать обновления программного обеспечения, включая программное обеспечение средств защиты информации
Владеть	- Основными средствами обеспечения безопасности данных. - Навыками работы с нормативными документами по администрированию баз данных. - Средствами обеспечения безопасности данных. - Навыками разработки и администрирования базы данных. - Навыками организации безопасности систем баз данных. - Средствами обеспечения безопасности данных и АИС. - Навыками сопровождения функционирования системы защиты информации информационной системы в ходе ее эксплуатации - Навыками анализа инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий
ПК-26 способностью администрировать подсистему информационной безопасности автоматизированной системы	
Знать	─ Основные принципы работы системы информационной безопасности автоматизированной системы и всех ее подсистем; ─ Принципы администрирования системы информационной безопасности автоматизированной системы.
Уметь	─ Настраивать систему информационной безопасности автоматизированной системы; ─ Настраивать подсистемы системы информационной безопасности автоматизированной системы; ─ Самостоятельно администрировать систему информационной безопасности автоматизированной системы.
Владеть	─ Навыками работы с системой информационной безопасности автоматизированной системы; ─ Навыками работы с подсистемами системы информационной безопасности автоматизированной системы; ─ Навыками администрирования системы информационной безопасности автоматизированной системы.

ПК-27 способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	
Знать	─ Способы обработки исключительных ситуаций ─ Нормативные документы по стандартизации и сертификации программной защиты. ─ Цели и задачи разработки политики информационной безопасности ─ Методы и средства анализа достаточности мер по обеспечению ИБ ПО ─Порядок контроля (мониторинга) за обеспечением уровня защищенности информации
Уметь	─ Разрабатывать порядок эксплуатации программного обеспечения ─ Разрабатывать политику учетных записей для эксплуатации информации ресурсов и программного обеспечения ─ Проводить мониторинг и аудит защищенности ПО ─Осуществлять контроль за событиями безопасности и действиями пользователей в информационной системе
Владеть	─ Методами анализа достаточности мер по обеспечению ИБ процессов создания и эксплуатации ПО ─ Методами контроля соблюдения политики учетных записей ─ Навыками регламентации обслуживания и осуществления модификации программного обеспечения
ПК-28 способностью управлять информационной безопасностью автоматизированной системы	
Знать	-методы и средства контроля охраняемых сведений - программные средства, поддерживающие управление информационной безопасностью -отечественный и зарубежный опыт в области управления информационной безопасностью - основные принципы создания системы управления информационной безопасностью
Уметь	-разрабатывать политики безопасности для элементов системы ОУ -расследовать инциденты ИБ -разрабатывать комплекс мероприятий по предотвращению инцидентов ИБ -готовить предложения для актуализации организационных мер по защите информационных систем - разрабатывать профили защиты
Владеть	- терминологией и процессным подходом построения СУИБ. -навыками определения актуальных угроз и применения мер их нейтрализации - навыками составления технических политик безопасности

6. Структура и содержание практики

Общая трудоемкость практики составляет 6 зачетных единиц 216 акад. часов, в форме практической подготовки 216 акад. часов**,** в том числе:
– контактная работа – 2,5 акад. часов:
– внеаудиторная – 2,5 акад. часов
– самостоятельная работа – 213,5 акад. часов;

№ п/п	Разделы (этапы) и содержание практики	Семестр	Виды работ на практике, включая самостоятельную работу	Код компетенции
1.	Подготовительный (ознакомительный)	8	Инструктаж по технике безопасности. Прослушивание вводного инструктажа по охране труда и изучение спецкурса в рамках образовательной программы. Получение индивидуальных заданий. Изучение требования по оформлению отчетности и защиты отчетов по практике.	ПСК-7.1, ПСК-7.2, ПСК-7.3, ПСК-7.4, ПСК-7.5, ОПК-3, ОПК-6, ОПК-8, ПК-3, ПК-4, ПК-5, ПК-6, ПК-7, ПК-8, ПК-9, ПК-10, ПК-11, ПК-12, ПК-13, ПК-14, ПК-15, ПК-16, ПК-17, ПК-18, ПК-19, ПК-20, ПК-21, ПК-22, ПК-23, ПК-24, ПК-25, ПК-26, ПК-27, ПК-28
2.	Экспериментально-исследовательский	8	Сбор фактического и литературного материала	ПСК-7.1, ПСК-7.2, ПСК-7.3, ПСК-7.4, ПСК-7.5, ОПК-3, ОПК-6, ОПК-8, ПК-3, ПК-4, ПК-5, ПК-6, ПК-7, ПК-8, ПК-9, ПК-10, ПК-11, ПК-12, ПК-13, ПК-14, ПК-15, ПК-16, ПК-17, ПК-18, ПК-19, ПК-20, ПК-21, ПК-22, ПК-23, ПК-24, ПК-25, ПК-26, ПК-27, ПК-28
3.	Обработка и анализ полученной информации.	8	Обработка и систематизация фактического и литературного материала. Подготовка отчета	ПСК-7.1, ПСК-7.2, ПСК-7.3, ПСК-7.4, ПСК-7.5, ОПК-3, ОПК-6, ОПК-8, ПК-3, ПК-4, ПК-5, ПК-6, ПК-7, ПК-8, ПК-9, ПК-10, ПК-11, ПК-12, ПК-13, ПК-14, ПК-15, ПК-16, ПК-17, ПК-18, ПК-19, ПК-20, ПК-21, ПК-22, ПК-23, ПК-24, ПК-25, ПК-26, ПК-27, ПК-28
4.	Отчетный	8	Подготовка и защита итогового отчета	ПСК-7.1, ПСК-7.2, ПСК-7.3, ПСК-7.4, ПСК-7.5, ОПК-3, ОПК-6, ОПК-8, ПК-3, ПК-4, ПК-5, ПК-6, ПК-7, ПК-8, ПК-9, ПК-10, ПК-11, ПК-12, ПК-13, ПК-14, ПК-15, ПК-16, ПК-17, ПК-18, ПК-19, ПК-20, ПК-21, ПК-22, ПК-23, ПК-24, ПК-25, ПК-26, ПК-27, ПК-28

7 Оценочные средства для проведения промежуточной аттестации по практике

Промежуточная аттестация по практике имеет целью определить степень достижения запланированных результатов обучения и проводиться в форме зачета с оценкой.

Обязательной формой отчетности обучающегося по практике является письменный отчет. Цель отчета – сформировать и закрепить компетенции, приобретенные обучающимся в результате освоения теоретических курсов и полученные им при прохождении практики. Отчеты обучающихся по практикам позволяют руководителям образовательных программ создавать механизмы обратной связи для внесения корректив в образовательный процесс.

Примерная структура и содержание раздела:

Промежуточная аттестация по производственной практике по получению профессиональных умений и опыта профессиональной деятельностиимеет целью определить степень достижения запланированных результатов обучения и проводиться в форме зачета с оценкой.

Зачет с оценкой выставляется обучающемуся за подготовку и защиту отчета по практике.

Подготовка отчета выполняется обучающимся самостоятельно под руководством преподавателя. При написании отчета обучающийся должен показать свое умение работать с нормативным материалом и литературными источниками, а также возможность систематизировать и анализировать фактический материал и самостоятельно творчески его осмысливать.

Содержание отчета определяется индивидуальным заданием, выданным руководителем практики. В процессе написания отчета обучающийся должен разобраться в теоретических вопросах избранной темы, самостоятельно проанализировать практический материал, разобрать и обосновать практические предложения.

На протяжении всего периода прохождения практики обучающийся должен вести дневник по практике, который будет являться приложением к отчету.

Примерное содержание отчета должно включать следующие разделы:

1. Титульный лист.
2. Аннотация.
3. Содержание.
4. Раздел 1.
5. Раздел 2.
6. Заключение.
7. Список использованных источников.

Титульный лист отчета оформляется в соответствии с СМК-О-ПВД-01-16. Аннотация отчета по производственной практике по получению профессиональных умений и опыта профессиональной деятельности должна содержать краткую характеристику отчета. В разделе 1 должен включать краткое описание учреждения, где проходила практика, основы организации его деятельности, вопросы информационной безопасности и техники безопасности. В разделе 2 описывается тема индивидуального задания.

Готовый отчет сдается на проверку преподавателю не позднее 3-х дней до окончания практики. Преподаватель, проверив отчет, может возвратить его для доработки вместе с письменными замечаниями. Обучающийся должен устранить полученные замечания и публично защитить отчет.

Примерное индивидуальное задание на производственную практику по получению профессиональных умений и опыта профессиональной деятельности:

Цель прохождения практики:

– закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника;

– 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.

Задачи практики:

– ознакомиться с нормативно-правовой документацией организации;

– изучить структуру организации;

– изучить и провести анализ должностных инструкций сотрудников организации;

– изучить и провести анализ решений по обеспечению ИБ предприятия;

– изучить и провести анализ методов контроля за исполнением принятых решений;

– проведение статистических исследований;

– изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты;

Вопросы, подлежащие изучению:

1) Род деятельности предприятия, на котором проходила практика.
2) Какие способы защиты информации используются на предприятии?
3) Какие программные средства используются для обеспечения информационной безопасности на предприятии?
4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности?
5) Какая топология используется в локальных сетях на предприятии?
6) Как обеспечивается безопасность беспроводных сетей?
7) Как обеспечивается безопасность по виброакустическим каналам передачи информации?
8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии.
9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей.
10) Опишите способы контроля трафика по локальным сетям предприятия.
11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть.
12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети?
13) При помощи, каких программных средств осуществляется администрирование ПК персонала предприятия?

14) Какие операционные системы используются на ПК персонала предприятия?
15) Какие операционные системы используются на серверах предприятия?
16) Понятие и виды защищаемой информации по законодательству РФ.
17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки.
18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну.
19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности.
20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации.
21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации.
22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права.
23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации).
24) Основное содержание разработки Политики безопасности предприятия (организации).
25) Принципы, основные задачи и функции обеспечения информационной безопасности.
26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации.
27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну.
28) Ответственность за нарушение законодательства в информационной сфере.
29) Основные мероприятия по защите информации при проведении совещаний и переговоров.
30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных).
31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников.
32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП).
33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации.
34) Сформулировать основные правила безопасной работы в компьютерной системе.
35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД.
36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты.
37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам.
38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения.
39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики.
40) Рассмотреть особенности разграничения доступа и аудита в СЗИ
41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа.
42) Раскрыть особенности образования электромагнитных каналов утечки информации.

43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации.
44) Сформулировать основные особенности построения периметровой охраны особо важных объектов

Планируемые результаты практики:

– подготовка рекомендаций по устранению или минимизации выявленных проблем (рекомендации должны быть обоснованными, т.е. сопровождаться ссылками на соответствующие НПА или авторитетное мнение специалистов в сфере деятельности, исследователей, конкурентов, потребителей и т.п.);

– подготовка выводов о деятельности предприятий или организаций, востребованности их продуктов на соответствующих рынках, а также практических рекомендаций по совершенствованию организационных и экономических аспектов их деятельности;

– оценка эффективности проектов и программ, внедряемых на предприятиях;

– оценка качества решений по обеспечению ИБ предприятия;

– публичная защита своих выводов и отчета по практике;

– систематизация и обобщение материала для написания выпускной квалификационной работы.

Показатели и критерии оценивания:

– на оценку **«отлично»** (5 баллов) – обучающийся представляет отчет, в котором в полном объеме раскрыто содержание задания; текст излагается последовательно и логично с применением актуальных нормативных документов; в отчете дана всесторонняя оценка практического материала; используется творческий подход к решению проблемы; сформулированы экономически обоснованные выводы и предложения. Отчет соответствует предъявляемым требованиям к оформлению.

На публичной защите обучающийся демонстрирует системность и глубину знаний, полученных при прохождении практики; стилистически грамотно, логически правильно излагает ответы на вопросы; дает исчерпывающие ответы на дополнительные вопросы преподавателя; способен обобщить материал, сделать собственные выводы, выразить свое мнение, привести иллюстрирующие примеры.

– на оценку **«хорошо»** (4 балла) – обучающийся представляет отчет, в котором содержание раскрыто достаточно полно, материал излагается с применением актуальных нормативных документов, основные положения хорошо проанализированы, имеются выводы и экономически обоснованные предложения. Отчет в основном соответствует предъявляемым требованиям к оформлению.

На публичной защите обучающийся демонстрирует достаточную полноту знаний в объеме программы практики, при наличии лишь несущественных неточностей в изложении содержания основных и дополнительных ответов; владеет необходимой для ответа терминологией; недостаточно полно раскрывает сущность вопроса; отсутствуют иллюстрирующие примеры, обобщающее мнение студента недостаточно четко выражено.

– на оценку **«удовлетворительно»** (3 балла) – обучающийся представляет отчет, в котором содержание раскрыты слабо и в неполном объеме, выводы правильные, но предложения являются необоснованными. Материал излагается на основе неполного перечня нормативных документов. Имеются нарушения в оформлении отчета.

На публичной защите обучающийся демонстрирует недостаточно последовательные знания по вопросам программы практики; использует специальную терминологию, но допускает ошибки в определении основных понятий, которые затрудняется исправить самостоятельно; демонстрирует способность самостоятельно, но не глубоко, анализировать

материал, раскрывает сущность решаемой проблемы только при наводящих вопросах преподавателя; отсутствуют иллюстрирующие примеры, отсутствуют выводы.

– на оценку **«неудовлетворительно»** (2 балла) – обучающийся представляет отчет, в котором содержание раскрыты слабо и в неполном объеме, выводы и предложения являются необоснованными. Материал излагается на основе неполного перечня нормативных документов. Имеются нарушения в оформлении отчета. Отчет с замечаниями преподавателя возвращается обучающемуся на доработку, и условно допускается до публичной защиты.

На публичной защите обучающийся демонстрирует фрагментарные знания в рамках программы практики; не владеет минимально необходимой терминологией; допускает грубые логические ошибки, отвечая на вопросы преподавателя, которые не может исправить самостоятельно.

– на оценку **«неудовлетворительно»** (1 балл) – обучающийся представляет отчет, в котором очень слабо рассмотрены практические вопросы задания, применяются старые нормативные документы и отчетность. Отчет выполнен с нарушениями основных требований к оформлению. Отчет с замечаниями преподавателя возвращается обучающемуся на доработку, и не допускается до публичной защиты.

8 Учебно-методическое и информационное обеспечение практики

а) Основная литература:

1. Веселов, Г. Е. Менеджмент риска информационной безопасности: Учебное пособие / Веселов Г.Е., Абрамов Е.С., Шилов А.К. - Таганрог:Южный федеральный университет, 2016. - 107 с.: ISBN 978-5-9275-2327-5. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/997108 (дата обращения: 31.08.2020)

2.Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/422772 (дата обращения: 31.08.2020).

3. Дибров, М. В. Сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 1 : учебник и практикум для вузов / М. В. Дибров. — Москва : Издательство Юрайт, 2020. — 333 с. — (Высшее образование). — ISBN 978-5-9916-9956-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/452430 (дата обращения: 31.08.2020).

4. Дибров, М. В. Сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 2 : учебник и практикум для вузов / М. В. Дибров. — Москва : Издательство Юрайт, 2020. — 351 с. — (Высшее образование). — ISBN 978-5-9916-9958-7. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/453063 (дата обращения: 31.08.2020).

5. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2019. — 312 с. — (Специалист). — ISBN 978-5-9916-9043-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/437163 (дата обращения: 31.08.2020).

6. Бабенко, Л. К. Криптографическая защита информации: симметричное шифрование : учебное пособие для вузов / Л. К. Бабенко, Е. А. Ищукова. — Москва : Издательство Юрайт, 2019. — 220 с. — (Университеты России). — ISBN 978-5-9916-9244-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/437667 (дата обращения: 31.08.2020).

7. Зашита информации : учеб. пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3-е изд. - Москва : РИОР: ИНФРА-М, 2019. - 400 с. - (Высшее образование). - DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-16-106478-8. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1018901 (дата обращения: 31.08.2020)

б) Дополнительная литература:

1. Внуков, А. А. Защита информации в банковских системах : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2018. — 246 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-01679-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/414083 (дата обращения: 31.08.2020).

2. Душкин, А. В. Методологические основы построения защищенных автоматизированных систем: Монография / Душкин А.В. - Воронеж:Научная книга, 2016. - 76 с. ISBN 978-5-4446-0902-6. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/923295 (дата обращения: 31.08.2020)

МАКРООБЪЕКТЫ:

3. Баранкова И. И. Сетевая защита информации. Лабораторный практикум

[Электронный ресурс] : учебное пособие [для вузов] / И. И., Баранкова, Д.Н. Мазнин, У.В. Михайлова, М.В. Афанасьева ; Магнитогорский гос. технический ун-т им. Г. И. Носова. - Магнитогорск : МГТУ им. Г. И. Носова, 2019. - 1 CD-ROM. - Загл. с титул. экрана. - ISBN 978-5-9967-1605-0 URL: https://magtu.informsystema.ru/uploader/fileUpload?name=3824.pdf&show=dcatalogues/1/1530260/3824.pdf&view=true (дата обращения 31.08.2020)

4. Баранков В. В. Развертывание и настройка виртуальных сетей [Электронный ресурс] : учебное пособие [для вузов] / В. В. Баранков, И. И. Баранкова, У. В. Михайлова, О. Б. Калугина] ; МГТУ. - Магнитогорск : МГТУ, 2019. - 1 электрон. опт. диск (CD-ROM). - ISBN 978-5-9967-1305-9 URL: https://magtu.informsystema.ru/uploader/fileUpload?name=3813.pdf&show=dcatalogues/1/1529986/3813.pdf&view=true (дата обращения 31.08.2020)

5. Архитектура и принципы работы вычислительных систем [Электронный ресурс] : учебное пособие [для вузов] / В.В. Баранков, И.И. Баранкова, М.В. Афанасьева, М.В. Коновалов; Магнитогорский гос. технический ун-т им. Г. И. Носова. - Магнитогорск : МГТУ им. Г. И. Носова, 2019. - 1 CD-ROM. - Загл. с титул. экрана. - ISBN 978-5-9967-1306-6 URL : https://magtu.informsystema.ru/uploader/fileUpload?name=3924.pdf&show=dcatalogues/1/1530495/3924.pdf&view=true (дата обращения 31.08.2020)

6. Сетевая защита информации. Лабораторный практикум : учебное пособие [для вузов] / Д. Н. Мазнин [и др.] ; Магнитогорский гос. технический ун-т им. Г. И. Носова. - Магнитогорск : МГТУ им. Г. И. Носова, 2019. - 1 CD-ROM. - Загл. с титул. экрана. - URL: https://magtu.informsystema.ru/uploader/fileUpload?name=3824.pdf&show=dcatalogues/1/1530260/3824.pdf&view=true (дата обращения: 31.08.2020). - Макрообъект. - ISBN 978-5-9967-1605-0. - Текст : электронный. - Сведения доступны также на CD-ROM.

7. Баранкова, И. И. Михайлова У.В. , Лукьянов Г.И. Техническая защита информации. Лабораторный практикум [Электронный ресурс] : учебное пособие / МГТУ. - Магнитогорск : МГТУ, 2017. - 1 электрон. опт. диск (CD-ROM). URL : https://magtu.informsystema.ru/uploader/fileUpload?name=2935.pdf&show=dcatalogues/1/1134667/2935.pdf&view=true (дата обращения 31.08.2020)

8. Баранкова, И. И. Определение критически значимых ресурсов объекта защиты при составлении модели угроз информационной безопасности : учебное пособие / И. И. Баранкова, О. В. Пермякова ; МГТУ. - Магнитогорск : МГТУ, 2017. - 1 электрон. опт. диск (CD-ROM). - Загл. с титул. экрана. - URL: https://magtu.informsystema.ru/uploader/fileUpload?name=3323.pdf&show=dcatalogues/1/1138331/3323.pdf&view=true (дата обращения: 31.08.2020). - Макрообъект. - Текст : электронный. - ISBN 978-5-9967-1031-7. - Сведения доступны также на CD-ROM.

*РЕЖИМ ПРОСМОТРА МАКРООБЪЕКТОВ

1. Перейти по адресу электронного каталога https://magtu.informsystema.ru
2. Произвести авторизацию (Логин: Читатель1 Пароль: 111111)
3. Активизировать гиперссылку макрообъекта

*При открытии макрообъектов учитывайте настройки антивирусной защиты

в) Методические указания:

Методические указания по выполнению самостоятельных работ по производственной-практике (Приложение 1) .

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение

Наименование ПО	№ договора	Срок действия лицензии
MS Windows 7 Professional(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office 2007 Professional	№ 135 от 17.09.2007	бессрочно
7Zip	свободно распространяемое ПО	бессрочно
Oracle Virtual Box	свободно распространяемое ПО	бессрочно
MS Office Visio Prof 2002(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office Visio Prof 2003(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office Visio Prof 2007(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office Visio Prof 2010(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office Visio Prof 2013(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office Visio Prof 2016(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office Visio Prof 2019(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office Access Prof 2003(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office Access Prof 2007(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office Access Prof 2010(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office Access Prof 2013(для классов)	Д-1227-18 от 08.10.2018	11.10.2021

MS Office Access Prof 2016(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS SQL Server Management Studio	свободно распространяемое ПО	бессрочно
Oracle My SQL Workbench Community Edition	свободно распространяемое ПО	бессрочно
Oracle SQL Developer	свободно распространяемое ПО	бессрочно
Oracle SQL Developer Data Modeler	свободно распространяемое ПО	бессрочно
WordPress	свободно распространяемое ПО	бессрочно
LibreOffice	свободно распространяемое ПО	бессрочно
MS Visual Studio 2013 Professional (для класса)	Д-1227-18 от 08.10.2018	11.10.2021
MS Visual Studio Code	свободно распространяемое ПО	бессрочно
MS Visual Studio 2017 Community Edition	свободно распространяемое ПО	бессрочно
Adobe Reader	свободно распространяемое ПО	бессрочно
MS Windows 10 Professional (для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Windows Server(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
Браузер Mozilla Firefox	свободно распространяемое ПО	бессрочно
Браузер Yandex	свободно распространяемое ПО	бессрочно
PostgreSQL	свободно распространяемое ПО	бессрочно
MariaDB	свободно распространяемое ПО	бессрочно
MS Office 2003 Professional	№ 135 от 17.09.2007	бессрочно
FAR Manager	свободно распространяемое ПО	бессрочно
Linux Calculate	свободно распространяемое ПО	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Электронная база периодических изданий East View Information Services, ООО «ИВИС»	https://dlib.eastview.com/
Национальная информационно-аналитическая система – Российский индекс научного цитирования (РИНЦ)	URL: https://elibrary.ru/project_risc.asp
Поисковая система Академия Google (Google Scholar)	URL: https://scholar.google.ru/
Информационная система - Единое окно доступа к информационным ресурсам	URL: http://window.edu.ru/
Федеральное государственное бюджетное учреждение «Федеральный институт промышленной собственности»	URL: http://www1.fips.ru/
Российская Государственная библиотека. Каталоги	https://www.rsl.ru
Федеральный образовательный портал – Экономика. Социология. Менеджмент	http://ecsocman.hse.ru/
Университетская информационная система РОССИЯ	https://uisrussia.msu.ru
Международная наукометрическая реферативная и полнотекстовая база данных научных изданий «Web of science»	http://webofscience.com
Международная реферативная и полнотекстовая справочная база данных научных изданий «Scopus»	http://scopus.com
Международная база полнотекстовых журналов Springer Journals	http://link.springer.com/
Международная коллекция научных протоколов по различным отраслям знаний Springer Protocols	http://www.springerprotocols.com/
Международная база научных материалов в области физических наук и инжиниринга SpringerMaterials	http://materials.springer.com/
Международная база справочных изданий по всем отраслям знаний SpringerReference	https://www.springer.com/gp
Международная реферативная база данных по чистой и прикладной математике zbMATH	http://zbmath.org/
Международная реферативная и полнотекстовая справочная база данных научных изданий «Springer Nature»	https://www.nature.com/siteindex
Архив научных журналов «Национальный электронно-информационный концорциум» (НП НЭИКОН)	https://archive.neicon.ru/xmlui/
Информационная система - Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации ФСТЭК России	https://fstec.ru/normotvorcheskaya/tekhnicheskaya-zashchita-informatsii

Информационная система - Банк данных угроз безопасности информации ФСТЭК России	https://bdu.fstec.ru/

9 Материально-техническое обеспечение практики

Рабочее место обучающегося при прохождении практики должно соответствовать действующим санитарным и противопожарным нормам, а также требованиям техники безопасности при проведении учебных и научно-производственных работ.

Обучающимся должна быть обеспечена возможность доступа к информации, необходимой для выполнения задания по практике и написанию отчета.

Организации, учреждения и предприятия, а также учебно-научные подразделения Университета должны обеспечить рабочее место обучающегося компьютерным оборудованием в объемах, достаточных для достижения целей практики.

Аудитории для самостоятельной работы (компьютерные классы; читальные залы библиотеки) оснащены персональными компьютерами с пакетом MS Office, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета».

Материально-техническое обеспечение учебной практики по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности включает:

Комплекс радиомониторинга «Касандра К-6».

Комплекс радиомониторинга «Касандра К-21».

Анализатор спектра «АКС-1301».

Комплект оборудования для мониторинга информационной безопасности.

Комплект оборудования контроля доступа.

Комплект оборудования для построения сети ZigBee.

Комплект оборудования SECURITY-CISCO-3M.

Портативный поисковый комплекс амплитудной пеленгации «Касандра С6»

Система оценки защищенности технических средств от утечки информации по каналу побочных электромагнитных излучений и наводок (ПЭМИН) Сигурд

Программно-аппаратный комплекс для измерения параметров волоконно-оптических систем передачи и оценки защищенности оптических линий связи Лазурит

Фильтр сетевой помехоподавляющий «ЛФС-100-3Ф»

Генератор шума ГШ-1000М.

Соната-АВ (модель 3М) система виброакустической и акустической защиты (Центральный ГШ): Генераторный блок (Модель 3М) + Аудиоизлучатель АИ-3М + «Тяжелый» виброизлучатель ВИ-3М + «Легкий» виброизлучатель ПИ-3М.

Устройство защиты Прокруст 2000.

Устройство КРИПТОН-ЗАМОК/У (АПМДЗ-У, М-526Б).

Устройства для защиты линий электропитания и заземления от утечки информации «Соната-РС2» исп. 208.

Комплект оборудования «Беспроводные компьютерные сети ЭВМ».

Модуль «Низкоуровневый контроллер Ethernet»

Комплект коммуникационного оборудования с сервером для моделирования облачного сервиса

Электронные ключи Guardant, eToken.

Комплект оборудования пользовательского сегмента системы GPS.

Комплект оборудования ТЛС-1.

Комплект оборудования VOIP.

Комплект оборудования «Кодирование и модуляция информации в системах связи».

Комплект оборудования «Исследование дистанционной передачи информации»

ПРИЛОЖЕНИЕ 1

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ВНЕАУДИТОРНЫХ САМОСТОЯТЕЛЬНЫХ РАБОТ

Общие положения

Настоящие методические указания предназначены для организации внеаудиторной самостоятельной работы обучающихся и оказания помощи в самостоятельном изучении теоретического и реализации компетенций обучаемых.

Данные методические указания не являются учебным пособием, поэтому перед началом выполнения самостоятельного задания следует изучить соответствующие разделы лекционных занятий, материалов образовательного портала, разделов основной и дополнительной литературы, представленных в пункте 8. «Учебно-методическое и информационное обеспечение дисциплины (модуля)» данной РПД.

Цели и задачи самостоятельной работы

Цель самостоятельной работы – содействие оптимальному усвоению материала обучающимися, развитие их познавательной активности, готовности и потребности в самообразовании.

Задачи самостоятельной работы:

- повышение исходного уровня владения информационными технологиями;
- углубление и систематизация знаний;
- постановка и решение стандартных задач профессиональной деятельности;
- развитие работы с различной по объему и виду информацией, учебной и научной литературой;
- практическое применение знаний, умений;
- самостоятельно использование стандартных программных средств сбора, обработки, хранения и защиты информации
- развитие навыков организации самостоятельного учебного труда и контроля за его эффективностью.

Показатели и критерии оценивания полученных знаний представлены в пункте 7.б) «Оценочные средства для проведения промежуточной аттестации» данной РПД.