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
«20» сентября 2017 г.

ПРОГРАММА ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

Направление подготовки (специальность)
10.05.03 Информационная безопасность автоматизированных систем
шифр наименование направления подготовки (специальности)

Направленность (профиль/ специализация) программы
Обеспечение информационной безопасности распределенных информационных систем
наименование направленности (профиля) подготовки (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 07.09.2018	
2.	8	Обновление списка основной и дополнительной литературы	№1 от 07.09.2018	
3.	7	Переработка фонда оценочных средств	№ 1 от 07.09.2019	
4.	8	Обновление списка основной и дополнительной литературы	№ 1 от 07.09.2019	
5.	7	Переработка фонда оценочных средств	№1 от 04.09.2020	
6.	8	Обновление списка основной и дополнительной литературы	№1 от 04.09.2020	

1 Цели производственной практики по получению профессиональных умений и опыта профессиональной деятельности

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 общепрофессионального 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.

2 Задачи производственной практики по получению профессиональных умений и опыта профессиональной деятельности

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 производственной практики по получению профессиональных умений и опыта профессиональной деятельности в структуре образовательной программы

Для прохождения производственной практики по получению профессиональных умений и опыта профессиональной деятельности необходимы знания, умения и владения, сформированные в результате изучения дисциплин математического и естественнонаучного цикла, профессионального цикла. Усвоение знаний, полученных студентами на производственной практике, призвано повысить их профессионализм и компетентность, а также способствовать развитию у студентов творческого мышления, системного подхода к построению информационных технологий на предприятиях и в организациях. Дисциплины «Информатика», «Теория информации», «Организация ЭВМ и вычислительных систем», «Языки программирования», «Техническая защита информации», «Программно-аппаратные средства обеспечения информационной безопасности», «Разработка и эксплуатация защищенных автоматизированных систем», «Разработка и эксплуатация защищенных автоматизированных систем», «Моделирование угроз информационной безопасности», «Методы выявления нарушений информационной безопасности, аттестация АИС» и «Сети и системы передачи информации» являются предшествующими производственной практике.

Знания, умения и владения, полученные в процессе прохождении производственной

практики по получению профессиональных умений и опыта профессиональной деятельности, будут необходимы для повышения их профессионализма и компетентности, а также способствует развитию у студентов творческого мышления, системного подхода к построению информационных технологий на предприятиях и в организациях.

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, систем контроля и мониторинга информационной безопасности и программно-аппаратной защиты средств вычислительной техники ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова», ООО «ММК-Информсервис», ПАО «Магнитогорский металлургический комбинат», ПНК удостоверяющий центр, и других предприятиях г. Магнитогорска, а также Управление ФСТЭК России по УрФО, г. Екатеринбург.

Способ проведения практики*: стационарная и/или выездная*

Производственная практика по получению профессиональных умений и опыта профессиональной деятельности осуществляется дискретно.

5 Компетенции обучающегося, формируемые в результате прохождения производственной практики по получению профессиональных умений и опыта профессиональной деятельности и планируемые результаты обучения

В результате прохождения производственной практики по получению профессиональных умений и опыта профессиональной деятельности у обучающего, должны быть сформированы следующие компетенции:

Структурный элемент компетенции	Планируемые результаты обучения
ОПК-3 Способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности	
Знать	- Язык программирования высокого уровня (объектно-ориентированное программирование); - Современные технологии и методы программирования; - Показатели качества программного обеспечения; - Методологии и методы проектирования программного обеспечения; - Методы тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования; - Принципы организации документирования разработки,процесса сопровождения программного обеспечения.
Уметь	- Работать с интегрированной средой разработки программного обеспечения; - Использовать динамически подключаемые библиотеки; - Реализовывать основные структуры данных и базовые алгоритмы средствами языков программирования; - Использовать шаблоны классов и средства макрообработки; - Проводить комплексное тестирование и отладку программных систем; - Проектировать и кодировать алгоритмы с соблюдением требований к

Структурный элемент компетенции	Планируемые результаты обучения
	качественному стилю программирования; - Проводить выбор эффективных способов реализации профессиональных задач; - Планировать разработку сложного программного обеспечения; - Формировать требования и разрабатывать внешние спецификациидля разрабатываемого программного обеспечения; автоматизированных систем;
Владеть	- Основными навыками проектирования программного обеспечения с использованием средств автоматизации. - Навыками программирования различными стилями. - Навыками разработки программной документации. - Навыками программирования с использованием эффективных реализаций структур данных и алгоритмов. - Навыками разработки, документирования, тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования.
ОПК-6 способностью применять нормативные правовые акты в профессиональной деятельности	
Знать	- Нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации. - Системы регулирования возникающих общественных отношений в информационной сферы. - Составляющие информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации. - Влияние информационной сферы на состояние политической, экономической, оборонной и других составляющих безопасности РФ.
Уметь	- Определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем. - Использовать инфраструктуру единого информационного пространства РФ в личных целях. - Определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем.
Владеть	- Методами разработки проектов нормативных документов, регламентирующих работу по защите информации. - Способами использования информационной инфраструктуры в интересах общественного развития. - Методами разработки проектов нормативных документов, регламентирующих работу по защите информации.
ОПК-8 способностью к освоению новых образцов программных, технических	

Структурный элемент компетенции	Планируемые результаты обучения
средств и информационных технологий	
Знать	- Классификацию современных программных и программно-аппаратных 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	- Основы методологии научных исследований. - Технические средства контроля эффективности мер защиты информации. - Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем - Классификацию современных компьютерных систем. - Современные способы использования компьютерных технологий для проведения исследований. - Технические средства контроля эффективности мер защиты информации. - Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем.
Уметь	- Пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет. - Анализировать основные узлы и устройства современных автоматизированных систем. - Пользоваться сетевыми информационными ресурсами для подбора необходимых современных компьютерных систем и правил работы в этих системах. - Эффективно использовать современные компьютерные технологии для изучения предмета исследования.
Владеть	- Представлением о возможности использования информационных технологий для решения профессиональных задач. - Представлением использования информационных технологий для проведения исследовательской работы в профессиональной деятельности. - Навыками пользования библиотеками прикладных программ для проведения исследовательской работы в профессиональной деятельности.

Структурный элемент компетенции	Планируемые результаты обучения
	- Представлением о способах и методах анализа защищенности информационной инфраструктуры автоматизированной системы.
ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	
Знать	- Основные источники угроз ИБ и факторы, необходимые для учета при разработке модели ИБ - классификацию угроз информационной безопасности - перечень нормативных документов - Способы реализации угроз безопасности информации и модели нарушителя в автоматизированных системах
Уметь	- анализировать и оценивать угрозы информационной безопасности объекта; - разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем выявлять уязвимости информационно-технологических ресурсов автоматизированных систем
Владеть	- Навыками определения информационной инфраструктуры и информационных ресурсов организации, подлежащих защите; - навыками семантического моделирования данных - методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем
ПК-5 способностью проводить анализ рисков информационной безопасности автоматизированной системы	
Знать	- методологию анализа рисков информационной безопасности - методики определения информационно-технологических ресурсов, подлежащих защите - способы применения анализа рисков в информационной безопасности при работе над междисциплинарными проектами - перечень информационно-технологических ресурсов, подлежащих защите способы применения анализа рисков в информационной безопасности при работе над инновационными проектами
Уметь	- применять терминологию анализа рисков информационной безопасности при работе над междисциплинарными и инновационными проектами - выполнять анализ особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите
Владеть	- терминологией, используемой при анализе особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите - навыками анализа особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите
ПК-6 способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере	

Структурный элемент компетенции	Планируемые результаты обучения
профессиональной деятельности	
Знать	- Основные информационные технологии, используемые в автоматизированных системах. - Сущность и понятие информационной безопасности и характеристику ее составляющих. - Основные проблемы обеспечения безопасности информации в компьютерных и автоматизированных системах.
Уметь	- Пользоваться современной научно-технической информацией по рассматриваемым в рамках дисциплины проблемам и задачам. - Принимать участие в исследованиях и анализе современной научно-технической информации по информационной безопасности. - Анализировать современную научно-техническую информацию по информационной безопасности. - Определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе
Владеть	- Основными методами научного познания в области защиты информации. - Навыками участия в проведении исследовательских работ по информационной безопасности. - Профессиональной терминологией в области информационной безопасности. - Разрабатывать предложения по совершенствованию системы управления безопасностью информации в автоматизированных системах
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	- разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации; - применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности
Владеть	- способностью разрабатывать научно-техническую документацию
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

Структурный элемент компетенции	Планируемые результаты обучения
	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 создавать дополнительные средства защиты; - Осуществлять анализ и оптимизацию 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; 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	

Структурный элемент компетенции	Планируемые результаты обучения
автоматизированных систем в сфере профессиональной деятельности	
Знать	- Современные технологии программирования. - Области и особенности применения языков программированиявысокого уровня; - Основные виды интегрированных сред разработки программного обеспечения. - Основные методы эффективного кодирования. - Способы обработки исключительных ситуаций; - Современные технологии и методы программирования, предназначенные для создания прикладных программ.
Уметь	- Реализовывать на языке высокого уровня алгоритмы решенияпрофессиональных задач; Работать с основными средами интегрированной разработки программногообеспечения; - Проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения; - Реализовывать разработанную структуру классов для задач предметной области.
Владеть	- Навыками реализации алгоритмов на языкахпрограммирования высокого уровня; - Навыками пользования библиотеками прикладных программ для решения прикладных задач профессиональной области. - Технологиями программирования распределенных автоматизированных систем;Способностью использовать языки, системы и инструментальные средства разработки автоматизированных систем.
ПК-11 способностью разрабатывать политику информационной безопасности автоматизированной системы	
Знать	- задачи органов защиты государственной тайны и служб защиты информации на предприятиях; - систему организационных мер, направленных на защиту информации ограниченного доступа - нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа; - основные угрозы безопасности информации и модели нарушителя объекта информатизации; - правовые основы организации защиты ПДн и охраны результатов интеллектуальной деятельности; - принципы формирования политики ИБ организации;
Уметь	- разрабатывать модели угроз и модели нарушителя ОИ; - разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации; - разрабатывать предложения по совершенствованию системы управления ИБ АС.
Владеть	- навыками выявления угроз безопасности информации в АС;

Структурный элемент компетенции	Планируемые результаты обучения
	- владеть навыками разработки политик безопасности различных уровней.
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 технологии RPC; - способы организации обмена данными при помощи технологии RMC; - способы организации обмена данными при помощи очередей; - функционал платформы .Net в части организации обмена данными; - функционал Run-Time Engine; - криптографические протоколы обмена информацией;
Уметь	- разрабатывать программное обеспечение по технологии Socket с учетом возможных состояний передающей, приемной сторон и линии связи;
Владеть	- навыками оформления программной документации по ЕСПД;
ПК-14 способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	
Знать	- Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах Классификацию криптографических средств защиты информации. - методы шифрования, использующие классические симметричные алгоритмы, - методы шифрования, использующие классические алгоритмы моноалфавитной и многоалфавитной подстановки и перестановки для защиты текстовой информации, - методы шифрования (расшифрования) перестановкой символов, подстановкой, гаммированием, использованием таблицы Виженера. - общие принципы действия шифровальной машины Энигма - общие принципы шифрования, используемые в алгоритме симметричного шифрования AES - принципы шифрования информации с помощью биграммного шифра Плейфера - Способы контрольных проверок работоспособности применяемых криптографических средств защиты информации.

Структурный элемент компетенции	Планируемые результаты обучения
Уметь	- исследовать различные методы защиты текстовой информации и их стойкости на основе подбора ключей - Участвовать в настройке криптографических средств обеспечения информационной безопасности. - Самостоятельно настраивать криптографические средства обеспечения ИБ. Исследовать эффективность контрольных проверок работоспособности применяемых криптографических средств ЗИ. - Применять криптографические средства обеспечения ИБ. Исследовать эффективность контрольных проверок работоспособности применяемых криптографических средств обеспечения ИБ.
Владеть	- Техникой настройки криптографических средств обеспечения информационной безопасности. - Навыками использования криптографических 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.
ПК-15 способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем	
Знать	- Модель жизненного цикла и порядок создания АС; - структуру, порядок составления, оформления и утверждения Технического задания по созданию АС - Общую характеристику и структуру стандартов по безопасности информационных технологий, виды требований безопасности, общую характеристику структуры классов и семейств функциональных требований безопасности к изделиям ИТ, общую характеристику классов требований доверия безопасности и структуры оценочных уровней доверия
Уметь	- Анализировать и оценивать угрозы информационной безопасности объекта - Определять потребности в технических средствах защиты и контроля - Планировать индивидуально-групповою структуру пользователей информационных систем и структуру разделяемых (коллективных) информационных ресурсов - Разрабатывать требования по защите компьютерных систем отображать предметную область на конкретную модель данных - Определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем - Выбирать меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы
Владеть	- методиками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем

Структурный элемент компетенции	Планируемые результаты обучения
	- навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем - практическими навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем
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 ВП по требованиям безопасности информации.
Уметь	– Принимать участие в исследованиях аттестации системы защиты информации; – Принимать участие в исследованиях и анализе аттестации системы защиты информации; – Проводить научно-исследовательские работы при аттестации системы защиты информации с учетом требований к обеспечению информационной безопасности.
Владеть	– Навыками использования средств анализа информационной безопасности; – Навыками участия в проведении экспериментально-исследовательских работ при аттестации АС с учетом требований к обеспечению информационной безопасности; – Навыками проведения аудита уровня защищенности и аттестацию информационных систем в соответствии с существующими нормами.
ПК-17 способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	
Знать	- Классификацию технических средств перехвата информации - Возможности технических средств перехвата информации - Организацию защиты информации от утечки по техническим каналам на объектах информатизации.
Уметь	- Классифицировать технические средства перехвата информации. - Участвовать в организации защиты информации от утечки по техническим каналам на объектах информатизации - Самостоятельно организовывать защиту информации от утечки по техническим каналам на объектах информатизации.
Владеть	- Средствами технической защиты информации. - Методами технической защиты информации. - Методами и средствами технической защиты информации.
ПК-18 способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности	
Знать	- Основные меры по защите информации в автоматизированных системах. - Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем. - Руководящие и методические документы уполномоченных

Структурный элемент компетенции	Планируемые результаты обучения
	федеральных органов исполнительной власти по защите информации. - Принципы организации работы малых коллективов исполнителей.
Уметь	- Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности. - Классифицировать и оценивать угрозы информационной безопасности для объекта информатизации. - Определять виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации.
Владеть	- Профессиональной терминологией в области информационной безопасности. - Навыками участия в проведении исследовательских работ по информационной безопасности. - Методами синтеза структурных и функциональных схем защищенных автоматизированных систем.
ПК-19 способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы	
Знать	- нормативные методические документы ФСТЭК России в области ИБ; - основные угрозы безопасности информации и модели нарушителя в ИС; - стратегии обеспечения ИБ, способы их организации и оптимизации.
Уметь	- оценивать различные инструменты в области проектирования и управления ИБ; - 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.
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. - Методики проектирования АС в защищенном исполнении.
Уметь	- Реализовывать разработанную автоматизированную систему с учетом требований ИБ. - Организовывать реализацию 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.
Владеть	- Навыками разработки автоматизированных систему с учетом требований ИБ. - Навыками контроля разработки АС с учетом требований ИБ.

Структурный элемент компетенции	Планируемые результаты обучения
	- Навыками контроля эффективности применения разработанной АС в защищенном исполнении. - Навыками разработки сопроводительной документации к разработанной АС в защищенном исполнении.
ПК-21 способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	
Знать	- основные меры по защите информации в автоматизированных системах (организационные, правовые); - автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности
Уметь	- разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации; оценивать автоматизированную систему как объект информационного воздействия - разрабатывать предложения по совершенствованию системы управления ИБ
Владеть	- методами организации и управления деятельностью служб защиты информации на предприятии
ПК-22 способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	
Знать	- основные угрозы безопасности информации и модели нарушителя ОИ; - правовые основы организации защиты ПДн и охраны результатов интеллектуальной деятельности; - принципы формирования политики информационной безопасности организации.
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 выявления угроз безопасности информации в АС; - владеть навыками разработки политик безопасности различных уровней.
ПК-23 способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	
Знать	- правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной системы - критерии оценки эффективности и надежности средств защиты операционных систем; специализированные средства выявления уязвимостей сетей ЭВМ;
Уметь	- реализовывать политику безопасности операционной системы; - сформировать комплекс мер для обеспечения информационной

Структурный элемент компетенции	Планируемые результаты обучения
	безопасности автоматизированной системы;
Владеть	- навыками формальной постановки задачи обеспечения информационной безопасности объектов информатизации. - навыками эксплуатации операционных систем и локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности; - навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем;
ПК-24 способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	
Знать	- основные понятия предметной области построения систем организационного управления - принципы построения и функционирования, примеры реализаций систем организационного управления; - основные критерии оценки защищенности систем организационного управления, источники угроз и нормативные документы - основные информационные технологии, используемые в автоматизированных системах; - нормативные правовые акты в области защиты информации - возможности, классификацию и область применения макрообработки;
Уметь	- применять при решении прикладных управленческих задач современные информационные технологии для поиска, прохождения, обработки, учета и рассылки информации внутри систем организационного управления - моделировать потоки информации, документооборот и бизнес-процессы, выполняемые в экономических системах с использованием средств Case-технологии и осуществлять их оценивание - разрабатывать техническую документацию для систем организационного управления - готовить научно-технические отчеты, обзоры, публикации по теме предметной области
Владеть	- навыками разработки технической документации для систем организационного управления - навыками подготовки научно-технических отчетов, обзоров, публикаций по теме предметной области - основами моделирования потоков информации, документооборота и бизнес-процессов в системах организационного управления
ПК-25 способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций	
Знать	- иметь представление об основных средствах защиты информационно-технологических ресурсов автоматизированной системы; - критерии защищенности ОС и сети ЭВМ;

Структурный элемент компетенции	Планируемые результаты обучения
	- средства защиты сетей ЭВМ; о современных средствах защиты информационно-технологических ресурсов автоматизированной системы; - критерии оценки эффективности и надежности средств защиты операционных систем; - принципы организации и структуру подсистем защиты операционных систем семейств UNIX и Windows;
Уметь	- использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем; - проводить мониторинг угроз безопасности компьютерных сетей, обеспечивать защиту сетевых подключений средствами операционной системы;
Владеть	- профессиональной терминологией в области информационной безопасности; - навыками работы с конкретными программными и аппаратными продуктами средств телекоммуникаций, удаленного доступа и сетевыми ОС; - навыками конфигурирования средств защиты информации; - навыками противодействия угрозами типа «недоверенная загрузка (НДЗ) операционной системы» и несанкционированный доступ (НСД) к операционной системе и вычислительной сети;
ПК-26 способностью администрировать подсистему информационной безопасности автоматизированной системы	
Знать	– Основные принципы работы системы информационной безопасности автоматизированной системы; – Основные принципы работы всех подсистем системы информационной безопасности автоматизированной системы; – 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	

Структурный элемент компетенции	Планируемые результаты обучения
Знать	- Принципы построения современных защищенных распределенных АС. - Способы разработки политики безопасности распределенных ИС. - Нормативные документы по стандартизации и сертификации программной защиты. - Способы управления разработкой политики безопасности распределенных ИС. - Методы и средства анализа достаточности мер по обеспечению ИБ процессов создания и эксплуатации защищенных распределенных АС.
Уметь	- Разрабатывать частные политики безопасности распределенных ИС. - Проводить мониторинг и аудит защищенности информационно-технологических ресурсов распределенных ИС. - Руководить разработкой и реализацией частных политики безопасности РИС. - Осуществлять мониторинг и аудит безопасности АС.
Владеть	- Методиками анализа политики безопасности РИС. - Методиками разработки политики безопасности РИС. - Методами анализа достаточности мер по обеспечению ИБ процессов создания и эксплуатации защищенных распределенных АС. - Методиками руководства разработкой политики безопасности РИС. - Методами обеспечения требований по ИБ процессов создания и эксплуатации защищенных РАС.
ПК-28 способностью управлять информационной безопасностью автоматизированной системы	
Знать	- основные угрозы безопасности информации и модели нарушителя в ИС; - основные меры по ЗИ в АС.
Уметь	- разрабатывать нормативно-методические материалы по регламентации системы организационной ЗИ; - расследовать инциденты ИБ.
Владеть	- навыками составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения ЗИ в АС; - терминологией и процессным подходом построения СУИБ.
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 - Выявление угроз безопасности информации в автоматизированных системах
Уметь	- Оценивать информационные риски в автоматизированных системах - Обнаруживать нарушения правил разграничения доступа - Классифицировать и оценивать угрозы безопасности информации - Определять подлежащие защите информационные ресурсы автоматизированных систем

Структурный элемент компетенции	Планируемые результаты обучения
	- Анализировать изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации
Владеть	- методами выявления угроз безопасности информации в автоматизированных системах - методами оценки последствий от реализации угроз безопасности информации в автоматизированной системе
ПСК-7.2 способностью проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах	
Знать	- о политиках безопасности и мерах защиты в распределённых приложениях - способы обеспечения информационной безопасности систем организационного управления - Методы и средства определения технологической безопасности функционирования распределенной информационной системы - методы и процедуры выявления угроз информационной безопасности в защищённых распределённых приложениях
Уметь	- формулировать основные требования к методам и средствам защиты информации в защищённых распределённых приложениях - 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
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.
Уметь	– Выявлять уязвимости информационно-технологических ресурсов автоматизированных систем; – Участвовать в проведении мониторинга угроз безопасности автоматизированных систем; – Самостоятельно проводить мониторинг угроз безопасности автоматизированных систем.
Владеть	– Методами выявления угроз информационной безопасности автоматизированных систем; – Методами мониторинга и аудита угроз информационной безопасности автоматизированных систем; – Методами мониторинга и аудита, выявления угроз информационной

Структурный элемент компетенции	Планируемые результаты обучения
	безопасности автоматизированных систем.
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;
Уметь	- разрабатывать и администрировать базы данных и интерфейсы прикладных программ к базам данных; - выделять сущности и связи предметной области; - выполнять запросы к базе данных; - нормализовывать отношения при проектировании реляционной базы данных; - создавать объекты базы данных;
Владеть	- методиками безопасной работы с БД с помощью современных образцов программных, технических средств; -в полной мере средствами администрирования БД в интегрированных средах СУБД.
ПСК-7.5 способностью координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении	
Знать	- руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации -основные вопросы организации организационного управления, виды и признаки классификации, основные требования стандартизации и унификации документов, способствующие повышению эффективности функционирования системы управления организацией -современные технологии и основные характеристики систем организационного управления, представленных на российском рынке -методы и средства проектирования систем организационного управления - методы и средства моделирования и оптимизации документооборота и бизнес-процессов автоматизации контроля исполнения и анализа их с целью дальнейшего совершенствования -организационные меры по защите информации
Уметь	-выбирать методы и подходы к проектированию СЭДО на предприятии; -разрабатывать постановку задачи и выбирать методы и средства построения системы преобразования бумажных документов в электронную форму, ввода их в электронный архив, организации хранения и поиска документов, формирования отчетов о работе системы -выявлять особенности и формировать требования к системе организации коллективной работы с документами в режиме совместного доступа и передачи их на исполнение по электронной почте или по локальной сети; -выполнять настройки систем планирования маршрутов передвижения

Структурный элемент компетенции	Планируемые результаты обучения
	документов и контролировать их исполнение
Владеть	-навыками подготовки научно-технических отчетов, обзоров, публикаций по теме предметной области -основами моделирования потоков информации, документооборота и бизнес-процессов -навыками администрирования систем организационного управления

6 Структура и содержание производственной практики по получению профессиональных умений и опыта профессиональной деятельности

Общая трудоемкость практики составляет 6 зачетных единицы, 216 акад. часов, в форме практической подготовки 216 акад. часов**,** том числе:

– контактная работа 2,5 акад. часов;

– самостоятельная работа 213,5 акад. часов.

Форма аттестация: дифференцированный зачет(зачет с оценкой)

№ п/п	Разделы (этапы) и содержание практики	Виды работ на практике, включая самостоятельную работу	Код и структурный элемент компетенции
1	подготовительный (ознакомительный)	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.	*ОПК-3 - з* *ОПК-6- з* *ОПК-8- з* *ПК-3- з* *ПК-4- з* *ПК-5- з* *ПК-6- з* *ПК-7- з* *ПК-8- з* *ПК-9- з* *ПК-10- з* *ПК-11- з* *ПК-12- з* *ПК-13- з* *ПК-14- з* *ПК-15- з* *ПК-16- з* *ПК-17- з* *ПК-18- з* *ПК-19- з* *ПК-20- з* *ПК-21- з* *ПК-22- з* *ПК-23- з* *ПК-24- з* *ПК-25- з*

№ п/п	Разделы (этапы) и содержание практики	Виды работ на практике, включая самостоятельную работу	Код и структурный элемент компетенции
			ПК-26- з *ПК-27- з* *ПК-28- з* *ПСК-7.1- з* *ПСК-7.2- з* *ПСК-7.3- з* *ПСК-7.4- з* *ПСК-7.5- з*
2	Экспериментально-исследовательский	сбор фактического и литературного материала	*ОПК-3 - зув* *ОПК-6- зув* *ОПК-8- зув* *ПК-3- зув* *ПК-4- зув* *ПК-5- зув* *ПК-6- зув* *ПК-7- зув* *ПК-8- зув* *ПК-9- зув* *ПК-10- зув* *ПК-11- зув* *ПК-12- зув* *ПК-13- зув* *ПК-14- зув* *ПК-15- зув* *ПК-16- зув* *ПК-17- зув* *ПК-18- зув* *ПК-19- зув* *ПК-20- зув* *ПК-21- зув* *ПК-22- зув* *ПК-23- зув* *ПК-24- зув* *ПК-25- зув* *ПК-26- зув* *ПК-27- зув* *ПК-28- зув* *ПСК-7.1- зув* *ПСК-7.2- зув* *ПСК-7.3- зув* *ПСК-7.4- зув* *ПСК-7.5- зув*

№ п/п	Разделы (этапы) и содержание практики	Виды работ на практике, включая самостоятельную работу	Код и структурный элемент компетенции
3	обработка и анализ полученной информации	обработка и систематизация фактического и литературного материала. Подготовка отчета	*ОПК-3 - зув* *ОПК-6- зув* *ОПК-8- зув* *ПК-3- зув* *ПК-4- зув* *ПК-5- зув* *ПК-6- зув* *ПК-7- зув* *ПК-8- зув* *ПК-9- зув* *ПК-10- зув* *ПК-11- зув* *ПК-12- зув* *ПК-13- зув* *ПК-14- зув* *ПК-15- зув* *ПК-16- зув* *ПК-17- зув* *ПК-18- зув* *ПК-19- зув* *ПК-20- зув* *ПК-21- зув* *ПК-22- зув* *ПК-23- зув* *ПК-24- зув* *ПК-25- зув* *ПК-26- зув* *ПК-27- зув* *ПК-28- зув* *ПСК-7.1- зув* *ПСК-7.2- зув* *ПСК-7.3- зув* *ПСК-7.4- зув* *ПСК-7.5- зув*
4	Отчетный	Сдача зачета	*ОПК-3 - зув* *ОПК-6- зув* *ОПК-8- зув* *ПК-3- зув* *ПК-4- зув* *ПК-5- зув* *ПК-6- зув* *ПК-7- зув* *ПК-8- зув* *ПК-9- зув*

№ п/п	Разделы (этапы) и содержание практики	Виды работ на практике, включая самостоятельную работу	Код и структурный элемент компетенции
			ПК-10- зув *ПК-11- зув* *ПК-12- зув* *ПК-13- зув* *ПК-14- зув* *ПК-15- зув* *ПК-16- зув* *ПК-17- зув* *ПК-18- зув* *ПК-19- зув* *ПК-20- зув* *ПК-21- зув* *ПК-22- зув* *ПК-23- зув* *ПК-24- зув* *ПК-25- зув* *ПК-26- зув* *ПК-27- зув* *ПК-28- зув* *ПСК-7.1- зув* *ПСК-7.2- зув* *ПСК-7.3- зув* *ПСК-7.4- зув* *ПСК-7.5- зув*

7 Оценочные средства для проведения промежуточной аттестации по производственной практике по получению профессиональных умений и опыта профессиональной деятельности

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-01-14. 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 производственной практики по получению профессиональных умений и опыта профессиональной деятельности

а) Основная литература:

1. Правила устройства электроустановок [Текст]: Все действующие разделы ПУЭ-6 и ПУЭ-7. – Новосибирск: Сиб. унив. изд-во, 2010. – 464 с

2. Шаньгин, В.Ф. Комплексная защита информации в корпоративных системах: инфор-мации [Электронный ресурс]: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. - 592 с. - (Высшее образование). Режим доступа: http://znanium.com/bookread.php?book=402686 **.– Заглавие с экрана. –ISBN 978-5-8199-0411-4.**

3. Малюк, А. А. Введение в информационную безопасность [Текст]: учеб. пособие для вузов/ А. А. Малюк, В. С. Горбатов, В. И. Королев и др М. : Горячая линия–Телеком, 2011. .– 288 с.

4. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ре-сурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. Режим доступа: http://znanium.com/bookread.php?book=405000 **.– Заглавие с экрана - ISBN 978-5-369-01178-2.**

б)Дополнительная литература:

1. Правила, инструкции, нормы пожарной безопасности РФ. Сборник нормативных документов [Текст]. – Новосибирск: Сиб. унив. изд-во, 2010. –176 с.

2. Гришина, Н.В. Комплексная система защиты информации на предприятии [Текст]: учеб. пособие/ Н.В Гришина. – М.: ФОРУМ, 2010. – 256 с.

3. Малюк, А. А. Теория защиты информации. [Текст]: учеб. пособие. М. : Горячая ли-ния–Телеком, 2012.– 184 с. – ISBN 978-5-9912-0246-6

4. Петренко, С.А. Петренко А.А. - Аудит безопасности Intranet. ДМК Пресс, 2010 – 386 с. Доступ в электронную библиотеку.

5. Информационная безопасность и защита информации [Текст]: учеб. пособ. / Ю. Ю. Громов, В. О. Драчёв, О. Г. Иванова, Н. Г. Шахов. - Старый Оскол : ТНТ, 2010. – 384 с. - ISBN 978-5-94178-216-1.

в)Программное обеспечение и Интернет-ресурсы:

1. Журнал Information Security. Информационная безопасность: периодич. интернет-изд. URL: http://www.itsec.ru/articles2/allpubliks **– Загл. с экрана. Яз. рус.**

2. Журнал «Вопросы кибербезопасности»: периодич. интернет-изд. URL: http://cyberrus.com/ – Загл. с экрана. Яз. рус.

3. Государственная публичная научно-техническая библиотека России [Электронный ресурс] / – Режим доступа: http://www.gpntb.ru**, свободный.– Загл. с экрана. Яз. рус.**

4. Российская национальная библиотека. [Электронный ресурс] / –URL: http://www.nlr.ru**. – Загл. с экрана. Яз. рус.**

5. Компьтерра: все новости про компьютеры, железо, новые технологии, информацион-ные : периодич. интернет-изд. URL: http://www.computerra.ru/ **– Загл. с экрана. Яз. рус.**

9 Материально-техническое обеспечение производственной практики по получению профессиональных умений и опыта профессиональной деятельности «Материально-техническое обеспечение ПАО «ММК» позволяет в полном объеме реализовать цели и задачи производственной практике по получению профессиональных умений и опыта профессиональной деятельности и сформировать соответствующие компетенции.

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

Студентам 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 студента 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 производственной практики по получению профессиональных умений и опыта профессиональной деятельности включает:

Наименование лаборатории	Оснащение лаборатории
Лаборатория радиомониторинга и контроля утечек информации ауд. 226	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. 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» Комплекс средств защиты информации ViPNet: криптошлюз и межсетевой экран.

Лаборатория программно-аппаратных средств защиты информации ауд. 2124	Комплект коммуникационного оборудования с сервером для моделирования облачного сервиса Электронные ключи Guardant, eToken.
Лаборатория сетевой безопасности ауд. 309а	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»
Аудитории для самостоятельной работы (ауд. 132а): компьютерные классы; читальные залы библиотеки.	Персональные компьютеры с ПО: Операционная система MS Windows 7 (Microsoft Imagine Premium D-1227-18 от 08.10.2018 до 08.10.2021); Пакет MS Office 2007 (Microsoft Open License 42649837, бессрочная); Выход в Интернет и доступ в электронную информационно-образовательную среду университета.