МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске

Зам. директора по учебной работе
ИСТиД (филиал) СКФУ в г. Пятигорске
_____ М.В. Мартыненко
«__» _____ 2020 г.

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ПО ПРОИЗВОДСТВЕННОЙ ПРАКТИКЕ

ЭКСПЛУАТАЦИОННАЯ ПРАКТИКА

Направление подготовки	10.03.01 Информационная безопасность
Направленность (профиль)	Комплексная защита объектов информатизации
Квалификация выпускника	бакалавр
Форма обучения	Очная
Год начала обучения	2020
Изучается	в 8 семестре

СОГЛАСОВАНО:
Зав. выпускающей кафедрой систем управления и информационных технологий
_____ И.М. Першин
«__» _____ 2020 г.

Представитель работодателя:
начальник отдела технической защиты информации ЗАО «Контур-Сервис ТВ»
_____ А.С. Ермаков
«__» _____ 2020 г.
Рассмотрено УМК
Протокол №___ от «___»_____

Председатель УМК ИСТиД (филиал) СКФУ в г. Пятигорске
_____А.Б. Нарыжная

РАЗРАБОТАНО:
Зав. кафедрой систем управления и информационных технологий
_____ И.М. Першин
«__» _____ 2020 г.

Старший преподаватель кафедры систем управления и информационных технологий
_____ А.С. Ермаков
«__» _____ 2020 г.

Пятигорск, 2020

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске

Зам. директора по учебной работе
ИСТиД (филиал) СКФУ в г. Пятигорске
_____ М.В. Мартыненко
«__» _____ 201_ г.

ПРОГРАММА ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

ЭКСПЛУАТАЦИОННАЯ ПРАКТИКА

Направление подготовки	10.03.01 Информационная безопасность
Направленность (профиль)	Комплексная защита объектов информатизации
Квалификация выпускника	бакалавр
Форма обучения	Очная
Год начала обучения	2020
Изучается	в 8 семестре

СОГЛАСОВАНО:
Зав. выпускающей кафедрой систем управления и информационных технологий
_____ И.М. Першин
«__» _____ 2020 г.

Представитель работодателя:
начальник отдела технической защиты информации ЗАО «Контур-Сервис ТВ»
_____ А.С. Ермаков
«__» _____ 2020 г.

Рассмотрено УМК
Протокол №___ от «___»_____

Председатель УМК ИСТиД (филиал) СКФУ в г. Пятигорске
_____А.Б. Нарыжная

РАЗРАБОТАНО:
Зав. кафедрой систем управления и информационных технологий
_____ И.М. Першин
«__» _____ 2020 г.

Старший преподаватель кафедры систем управления и информационных технологий
_____ А.С. Ермаков
«__» _____ 2020 г.

Пятигорск, 2020

1. **Цели практики**

Целями эксплуатационной практики по направлению подготовки 10.03.01 Информационная безопасность являются:

- закрепление, расширение, углубление и систематизация знаний, полученных при изучении дисциплин профиля подготовки;
- приобретение практических навыков и компетенций в сфере профессиональной деятельности;
- подбор необходимого материала для выполнения для дальнейшей проработки темы выпускной квалификационной работы.

2. **Задачи практики**:

Задачами эксплуатационной практики являются:

1) Изучить:
- современные аппаратные и программные средства вычислительной техники;
- принципы организации информационных систем в соответствии с требованиями информационной защищенности и в соответствии с требованиями по защите государственной тайны;
- конструкцию и основные характеристики технических устройств хранения, обработки и передачи информации;
- потенциальные каналы утечки информации, способы их выявления и методы оценки опасности;
- основную номенклатуру и характеристики аппаратуры, используемой для перехвата и анализа сигналов в технических каналах утечки информации;
- методы и средства инженерно-технической защиты информации;
- принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;
- принципы построения современных криптографических систем, стандарты в области криптографической защиты информации;
- основные правовые положения в области информационной безопасности и защиты информации.

2) Освоить:
- методы организации и управления деятельности служб защиты информации на предприятии;
- технологии проектирования, построения и эксплуатации комплексных систем защиты информации;
- методы научных исследований уязвимости и защищенности информационных процессов;
- методики проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.

3) Подобрать, изучить и обобщить научно-техническую литературу, нормативно-методические материалы по инженерно-технической защите информации. Научиться внедрять комплексные системы и отдельные специальные технические и программно-математические средства защиты информации на объектах информатизации. Разработать предложения по совершенствованию и повышению эффективности применяемых мер на основе анализа результатов контрольных проверок, изучения и обобщения опыта эксплуатации объекта информатизации. Участвовать в проведении аттестации объектов, помещений, технических средств, программ, алгоритмов на предмет соответствия требованиям защиты информации по соответствующим классам безопасности. Знать

вопросы нормирования, организации и оплаты труда, вопросы обеспечения безопасности жизнедеятельности на предприятии.

3. Место практики в структуре образовательной программы

Эксплуатационная практика относится к блоку 2 «Практики», ее освоение происходит в 8-м семестре. Практика базируется на следующих дисциплинах. практиках: «Введение в теорию случайных процессов», «Администрирование в радиоканальных информационных системах», «Интегрированные распределенные системы охраны объектов», «Проектно-технологическая практика».

Для освоения программы практики, обучающиеся должны владеть следующими знаниями и компетенциями:

- способностью к самостоятельному обучению новым методам исследования, к изменению научного и научно-производственного профиля своей профессиональной деятельности;
- использованием на практике умений и навыков в организации исследовательских и проектных работ, в управлении коллективом.

Результаты прохождения практики могут быть использованы в дальнейшем в подготовке выпускных квалификационных работ.

4. Вид, тип практики, способ и формы ее проведения

Вид практики: производственная;
Тип практики: эксплуатационная;
Способ проведения практики: выездная или стационарная.
Форма проведения практики: непрерывно.

5. Место и время проведения практики

Эксплуатационная практика может проводиться в сторонних организациях или на кафедрах и в лабораториях вуза, обладающих необходимым кадровым и научно-техническим потенциалом.

Эксплуатационная практика проводится в 8 семестре, продолжительностью 2 недели.

6. Перечень планируемых результатов обучения при прохождении практики, соотнесенных с планируемыми результатами освоения образовательной программы

6.1 Наименование компетенций

Индекс	Формулировка:
ОК-5	способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики
ОК-8	способностью к самоорганизации и самообразованию
ПК-1	способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
ПК-2	способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач

ПК-3	способностью администрировать подсистемы информационной безопасности объекта защиты
ПК-4	способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты
ПК-5	способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации
ПК-8	способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов
ПК-9	способностью осуществлять подбор, изучение и обобщение научно- технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности
ПК-12	способностью принимать участие в проведении экспериментальных исследований системы защиты информации
ПК-13	способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации
ПК-14	способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности
ПК-15	способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
ПСК-1	способностью участвовать в разработке и эксплуатации подсистемы управления информационной безопасностью
ПСК-2	способностью применять современные информационные технологии и методы цифровой обработки сигналов для эффективного анализа и использования массивов информации при решении задач обеспечения информационной безопасности автоматизированных систем

6.2 Знания, умения, навыки и (или) опыт деятельности, характеризующие этапы формирования компетенций

Формируемые компетенции	Вид работы обучающегося на практике	Планируемые результаты обучения при прохождении практики, характеризующие этапы формирования компетенций		
		Навыки или практический опыт деятельности	Умения	Знания
ОК-5, ОК-8	Знакомство с коллективом организации, с его деятельностью и нормативными документами	Владеть методикой проверки защищенности объектов информатизации на соответствие требованиям	Обобщать научно-техническую литературу, нормативно-методические материалы по инженерно-	Знать вопросы нормирования, организации и оплаты труда, вопросы обеспечения безопасности жизнедеятельности

	Самостоятельное знакомство и анализ нормативных документов, связанных с защитой информации на данном предприятии	нормативных документов Владеть методикой исследования защищенности объектов информатизации от утечки информации	технической защите информации Подбирать, научно-техническую литературу по инженерно-технической защите информации	на предприятии. Знать основные правовые положения в области информационной безопасности и защиты информации
ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-8, ПК-9, ПК-12, ПК-13, ПК-14, ПК-15ПК-13, ПК-14, ПК-15	Знакомство с локальными документами, связанными с защитой информации на данном предприятии Составление краткого отчета об уровне защищенности данного предприятия от утечки информации	Владеть методикой изучения локальных документов защищенности объектов от утечки информации на предмет их соответствия нормативной документации Владеть методами составления обзора по вопросам обеспечения информационной безопасности	Оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, по профилю своей профессиональной деятельности	Знать рабочую техническую документацию с учетом действующих нормативных и методических документов. Знать методы и приемы подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов по профилю своей профессиональной
ПСК-1 ПСК-2	Разработать комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации, провести выбор необходимых технологий и технических средств, организовать	Владеть приемами выбора, организации внедренияи последующего сопровождение необходимых технологий и технических средств. Владеть приемами расчета экономической целесообразности проекта	Уметь разработать комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации Уметь внедрять комплексные системы и отдельные специальные технические и программно-математические	Знать принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации. Знать современные аппаратные и программные средства вычислительной техники

	его внедрение и последующее сопровождение Утвердить сформированный комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности с руководством организации		средства защиты информации на объектах информатизации.	

6.3.Соответствие планируемых результатов видам профессиональной деятельности

Планируемые результаты сформулированы в соответствии с профессиональным стандартом «Специалист по технической защите информации», утвержден приказом Министерства труда и социальной защиты Российской Федерации от «1» ноября 2016г. № 599н.

Виды профессиональной деятельности выпускника в соответствии с ОП	Задачи профессиональной деятельности выпускника	Трудовые функции	Вид работы студента на практике	Реализуемые компетенции (в соответствии с ОП)
	установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований	Проведение работ по установке и техническому обслуживанию средств защиты информации	разработать комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации	ОК-5, ОК-8, ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-8, ПК-9, ПК-12, ПК-13, ПК-14, ПК-15ПСК-1, ПСК-2
	администрирован	Проведение	организовать	ОК-5, ОК-

эксплуатационная	ие подсистем информационной безопасности объекта;	работ по установке и техническому обслуживанию защищенных технических средств обработки информации	внедрение комплекса мер по организации информационной безопасности и его последующее сопровождение	ОК-5, ОК-8, ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-8, ПК-9, ПК-12, ПК-13, ПК-14, ПК-15ПСК-1, ПСК-2
	участие в проведении аттестации объектов информатизации по требованиям безопасности информации и аудите информационной безопасности автоматизированных систем;	Проведение аттестации объектов на соответствие требованиям по защите информации	внедрять комплексные системы и отдельные специальные технические и программно-математические средства защиты информации на объектах информатизации	ПСК-5, ПСК-6
экспериментально-исследовательская	сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования;	Проведение аттестации объектов на соответствие требованиям по защите информации	знакомство с коллективом организации, с его деятельностью и нормативными документами	ОК-5, ОК-8
	проведение экспериментов по заданной методике, обработка и анализ их результатов;	Проведение аттестации объектов на соответствие требованиям по защите информации	проведение анкетирования работников организации с целью исследования системы защиты информации	ОК-5, ОК-8, ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-8, ПК-9, ПК-12, ПК-13, ПК-14, ПК-15ПСК-1, ПСК-2
	проведение вычислительных экспериментов с использованием стандартных программных средств;	Проведение сертификационных испытаний средств защиты информации на соответствие требованиям	обработка экспериментальных данных, полученных при анкетировании	ОК-5, ОК-8, ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-8, ПК-9, ПК-12, ПК-13, ПК-14, ПК-

		по безопасности информации		15ПСК-1, ПСК-2, ПСК-6
организационно-управленческая.	осуществление организационно-правового обеспечения информационной безопасности объекта защиты;	Организация и проведение работ по технической защите информации	расчет экономической целесообразности проекта	ПСК-6
	организация работы малых коллективов исполнителей;	Организация и проведение работ по технической защите информации	организация внедрения и последующего сопровождение разработанного проекта	ПСК-5
	участие в совершенствовании системы управления информационной безопасностью;	Организация и проведение работ по технической защите информации	внедрение комплексной системы и отдельных специальных технических и программно-математических средств защиты информации на объекте информатизации	ПСК-6
	изучение и обобщение опыта работы других учреждений, организаций и предприятий в области защиты информации, в том числе информации ограниченного доступа;	Организация и проведение работ по технической защите информации	знакомство с локальными документами, связанными с защитой информации на различных предприятиях определенной отрасли	ОК-5, ОК-8, ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-8, ПК-9, ПК-12, ПК-13, ПК-14, ПК-15ПСК-1, ПСК-2
	контроль эффективности реализации политики информационной безопасности объекта защиты.	Проведение аттестации объектов на соответствие требованиям по защите информации	изучение современных аппаратных и программных средства вычислительной техники	ОК-5, ОК-8, ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-8, ПК-9, ПК-12, ПК-13, ПК-14, ПК-15ПСК-1, ПСК-2

7. Объем практики

Объем занятий: Итого 81 ч. 3 з.е.
Продолжительность 2 недели
Дифференцированный зачет 8 семестр

8. Структура и содержание практики

Разделы (этапы) практики	Реализуемые компетенции	Виды работ обучающегося на практике	Количество часов	Формы текущего контроля
Начальный этап	ОК-5, ОК-8, ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-8, ПК-9, ПК-12, ПК-13, ПК-14, ПК-15ПСК-1, ПСК-2	Сбор, обработка и систематизация фактического материала Изучение организационно-правовой структуры объекта исследования. Анализ объекта исследования на предмет комплексной защиты информации.	27	
Промежуточный этап	ОК-5, ОК-8, ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-8, ПК-9, ПК-12, ПК-13, ПК-14, ПК-15ПСК-1, ПСК-2	Сбор, обработка и систематизация фактического и литературного материала Наблюдения, измерения Самостоятельная работа	27	
Заключительный этап	ОК-5, ОК-8, ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-8, ПК-9, ПК-12, ПК-13, ПК-14, ПК-15ПСК-1, ПСК-2	Составление отчета по практике Формирование предложений Публичная защита отчета	27	Публичная защита выполненной работы, по итогом, которой выставляется зачет с оценкой

9. Формы отчетности по практике

1. Дневник
2. Отчет обучающегося

3. Отзыв руководителя практики от вуза
   Структура отчета
   1. Задания

   _____

   _____

   2. Индивидуальное задание

   _____

   _____

   3. Список использованной литературы
   4. Приложения (при необходимости).

10. Технологическая карта самостоятельной работы обучающегося

Коды реализуемых компетенций	Вид деятельности обучающегося	Итоговый продукт самостоятельной работы	Средства и технологии оценки	Объем часов, в том числе		
				СРС	Контактная работа с преподавателем	Всего
ОК-5, ОК-8	Сбор материалов по структуре предприятия, правил документооборота	отчет	Собеседование	11	2	13
ПК-9, ПСК-1	Подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по инженерно-технической защите объектов информатизации	отчет	Устный опрос	11	2	13
ПК-8, ПК-12	проведение экспериментов по заданной методике, обработка и анализ результатов.	отчет	Собеседование	11	2	13
ПСК-1, ПСК-2	сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности.	отчет	Устный опрос	11	2	13
ПСК-2, ПСК-1	Предложения по совершенствованию системы управления информационной безопасностью.	отчет	Собеседование	11	2	13

ПСК-2, ПСК-1	Оформление отчёта по практике.	отчет	Защита отчета оценкой	14	2	16
Итого за 8 семестр				**69**	**12**	**81**
Итого				**69**	**12**	**81**

11. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по практике

Фонды оценочных средств, позволяющие оценить уровень сформированности компетенций, размещен в УМК производственно-технологической практики на кафедре Систем управления и информационных технологий и представлен следующими компонентами:

11.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы. Паспорт фонда оценочных средств

Код оцениваемой компетенции	Этап формирования компетенции	Средства и технологии оценки	Тип контроля	Вид контроля	Наименование оценочного средства
ОК-5, ОК-8, ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-8, ПК-9, ПК-12, ПК-13, ПК-14, ПК-15ПСК-1, ПСК-2	Начальный	собеседование	текущий	текущий	Задания для проверки уровня знаний
ОК-5, ОК-8, ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-8, ПК-9, ПК-12, ПК-13, ПК-14, ПК-15ПСК-1, ПСК-2	Промежуточный	Собеседование	текущий	текущий	Задания для проверки уровня умений и навыков
ОК-5, ОК-8, ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-8, ПК-9, ПК-12, ПК-13, ПК-14, ПК-15ПСК-1, ПСК-2	Заключительный	Защита отчета	промежуточный	промежуточный	Задания на практику

11.2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Уровни сформированности	Индикаторы	Дескрипторы			
		2 балла	3 балла	4 балла	5 баллов*

компетенций					
Базовый	**Знать:** принципы организации информационных систем в соответствии с требованиями информационной защищенности и в соответствии с требованиями по защите государственной тайны; потенциальные каналы утечки информации, способы их выявления и методы оценки опасности; основную номенклатуру и характеристики аппаратуры, используемой для перехвата и анализа сигналов в технических каналах утечки информации; методы и средства инженерно-технической защиты информации;	Отсутствует знания: принципов организации информационных систем в соответствии с требованиям информационной защищенности и в соответствии с требованиями по защите государственной тайны; потенциальных каналов утечки информации, способов их выявления и методы оценки опасности; основной номенклатуры и характеристик аппаратуры, используемой для перехвата и анализа сигналов в технических каналах утечки информации; методов и средств инженерно-технической защиты информации;	Имеются знания: принципов организации информационных систем в соответствии с требованиями информационной защищенности и в соответствии с требованиями по защите государственной тайны; потенциальных каналов утечки информации, способов их выявления и методы оценки опасности; - основной номенклатуры и характеристик аппаратуры, используемой для перехвата и анализа сигналов в технических каналах утечки информации методов и средств инженерно-технической защиты информации	Знает: принципы организации информационных систем в соответствии с требованиями информационной защищенности и в соответствии с требованиями по защите государственной тайны; потенциальные каналы утечки информации, способы их выявления и методы оценки опасности; основную номенклатуру и характеристики аппаратуры, используемой для перехвата и анализа сигналов в технических каналах утечки информации; методы и средства инженерно-технической защиты информации;	

	Уметь: подбирать, обобщать научно-техническую литературу, нормативно-методические материалы по инженерно-технической защите информации; внедрять комплексные системы и отдельные специальные технические и программно-математические средства защиты информации на объектах информатизации	Отсутствует умения: подбирать, обобщать научно-техническую литературу, нормативно-методические материалы по инженерно-технической защите инфор-мации; внедрять комплексные системы и отдельные специальные технические и программно-математически е средства защиты информации на объектах информатизаци и	Имеются умения: подбирать, обобщать научно-техническую литературу, нормативно-методически е материалы по инженерно-технической защите информации ; внедрять комплексны е системы и отдельные специальные технические и программно-математичес кие средства защиты информации на объектах информатиз ации	Умеет: подбирать, обобщать научно-техническую литературу, нормативно-методически е материалы по инженерно-технической защите информации; внедрять комплексные системы и отдельные специальные технические и программно-математическ ие средства защиты информации на объектах информатиза ции	
	Владеть: методами организации и управления деятельностью служб защиты информации на предприятии; технологией проектирования, построения и эксплуатации комплексных систем защиты информации;	Отсутствует навыки владения: методами организации и управления деятельностью служб защиты информации на предприятии; технологией проектировани я, построения и эксплуатации комплексных систем защиты информации	Имеются навыки владения: методами организации и управления деятельност ью служб защиты информации на предприя-тии; технологией проектирова ния, построения и эксплуатаци и комплексны	Владеет: методами организации и управления деятельность ю служб защиты информации на предприятии; технологией проектирован ия, построения и эксплуатации комплексных систем защиты информации;	

			х систем защиты информации		
Повышенный	**Знать:** принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; принципы построения современных криптографических систем, стандарты в области криптографической защиты информации; основные правовые положения в области информационной безопасности и защиты информации;				Знает: принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; принципы построения современных криптографических систем, стандарты в области криптографической защиты информации; основные правовые положения в области информационной безопасности и защиты информации
	Уметь: разрабатывать предложения по совершенствованию и повышению эффективности применяемых мер				Умеет: разрабатывать предложения по совершенствованию и повышению

	по защите информации, на основе анализа результатов контрольных проверок				эффективности применяемых мер на основе анализа результатов контрольных проверок
	Владеть: методикой проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.				Владеет: методикой проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.

11.3. Критерии оценивания компетенций

Оценка *«отлично»* выставляется студенту, если:

- знает, как решать практические задачи в области информационной безопасности и имеет практические навыки.
- знает, как решать практические задачи повышенной сложности в области информационной безопасностии имеет практические навыки.
- способен выполнять решения практических задач в области информационной безопасности в полном объеме, полностью способен к самостоятельному выполнению решения практических задач в области информационной безопасности.
- способен выполнять решения практических задач повышенной сложности в области информационной безопасностив полном объеме, полностью способен к самостоятельному выполнению решения практических задач в области информационной безопасности.

Оценка «*хорошо*» выставляется студенту, если:

- имеются знания практических задач в области информационной безопасности, но навыки реализуются недостаточно.
- имеются знания практических задач в области информационной безопасности, но навыки реализуются недостаточно.
- умеет решать практические задачи в области информационной безопасности.

Оценка «*удовлетворительно*» выставляется студенту, если:

- знания практических задач в области информационной безопасности имеются, но практических навыков нет.
- демонстрирует понимание значимости практических задач в области информационной безопасности. Испытывает затруднения в решении практических задач в области информационной безопасности.

– знания практических задач в области информационной безопасностиимеются, но практических навыков нет.

Оценка «*неудовлетворительно*» выставляется студенту, если:

– отсутствуют знания практических задач в области информационной безопасности.
– отсутствуют знания практических задач в области информационной безопасности.
– отсутствие способности для решения практических задач в информационной безопасности. Не умеет решать практические задачи в области информационной безопасности.

11.4. Описание шкалы оценивания

Максимальная сумма баллов по **практике** устанавливается в **100** баллов и переводится в оценку по 5-балльной системе в соответствии со шкалой:

Шкала соответствия рейтингового балла 5-балльной системе

Рейтинговый балл	**Оценка по 5-балльной системе**
88 – 100	Отлично
72 – 87	Хорошо
53 – 71	Удовлетворительно
<53	Неудовлетворительно

11.5 Типовые контрольные задания, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения ОП

Задания, позволяющие оценить знания, полученные на практике (базовый уровень)

Контролируемые компетенции или их части (код компетенции)	Формулировка задания	
Общекультурные компетенции (ОК):		
ОК-5 способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики;	Задание 1	Изучение норм охраны труда при проведении проектно-конструкторских работ
	Задание 2	Изучение рекомендаций по технике безопасности при проведении проектно-конструкторских работ
ОК-8 способностью к самоорганизации и самообразованию;	Задание 1	Изучение основных видов нормативно-правовой документации в сфере информационной безопасности.
	Задание 2	Изучение организационно-правовой документации предприятия (устав, положение о предприятии и т.д.)
Профессиональные компетенции (ПК):		
ПК-8 способностью оформлять рабочую техническую документацию с учетом действующих нормативных и	Задание 1	Изучение технической документации.
	Задание 2	Изучение методических документов по защите информации.

методических документов;		
ПК-9 способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;	Задание 1	Аудит информационной безопасности предприятия.
	Задание 2	Обзор современных средств защиты информации.
ПК-12 способностью принимать участие в проведении экспериментальных исследований системы защиты информации	Задание 1	Проведение анкетирования работников на предмет информационной безопасности предприятия.
	Задание 2	Первичная статистическая обработка анкет.
Профессиональные специальные компетенции (ПК):		
ПСК-1 способностью участвовать в разработке и эксплуатации подсистемы управления информационной безопасностью	Задание 1	Обзор технических средств и необходимых для их установки технологий.
	Задание 2	Изучение правил внедрения и адаптации систем безопасности.
ПСК-2 способностью применять современные информационные технологии и методы цифровой обработки сигналов для эффективного анализа и использования массивов информации при решении задач обеспечения информационной безопасности автоматизированных систем	Задание 1	Обзор программных средств и необходимых для их установки технологий.
	Задание 2	Изучение правил настройки систем безопасности.

Задании, позволяющие оценить знания, полученные на практике (повышенный уровень)

Контролируемые компетенции или их части		Формулировка задания	
Код компетенции	Формулировка		
Общекультурные компетенции (ОК):			
ОК-5 способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и		Задание 1	Разработка проекта охранной сигнализации на примере мастерской.
		Задание 2	Разработка проекта охранной сигнализации на примере расчетно-кассового центра.

государства, соблюдать нормы профессиональной этики;		
ОК-8 способностью к самоорганизации и самообразованию;	Задание 1	Разработка проекта охранной сигнализации на примере офисного помещения.
	Задание 2	Изучение должностных инструкций сотрудников, непосредственнозанятых вопросами защиты информации.
Профессиональные компетенции (ПК):		
ПК-8 способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов;	Задание 1	Изучение методов тестирования компонентов системпо защите информации.
	Задание 2	Изучение методик исследования защиты информации на предприятии.
ПК-9 способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;	Задание 1	Подробное изучение современных средств защиты информации.
	Задание 2	Разработка предложений по модернизации защиты информации на предприятии.
ПК-12 способностью принимать участие в проведении экспериментальных исследований системы защиты информации	Задание 1	Полная статистическая обработка анкет.
	Задание 2	Разработка предложений по программному обеспечению защиты информации.
Профессиональные специальные компетенции (ПК):		
ПСК-1 способностью участвовать в разработке и эксплуатации подсистемы управления информационной безопасностью	Задание 1	Изучение правил внедрения и адаптации современных систем безопасности.
	Задание 2	Изучение методов тестирования компонентов информационных систем.
ПСК-2 способностью применять современные информационные технологии и методы цифровой обработки сигналов для эффективного анализа и использования массивов информации при решении задач обеспечения информационной безопасности автоматизированных систем	Задание 1	Разработка проекта охранной сигнализации на примере 1-го этажа торгового центра.
	Задание 2	Разработка проекта охранной сигнализации на примере выставочного комплекса охранных систем.

Задания, позволяющие оценить умения и навыки, полученные на практике (базовый уровень)

Контролируемые компетенции	Формулировка задания

или их части			
Код компетенции	Формулировка		
Общекультурные компетенции (ОК):			
ОК-5 способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики;		Задание 1	Проведение аналитической работы по предупреждению утечки конфиденциальной информации.
		Задание 2	Составление рекомендаций по технике безопасности при проведении проектно-конструкторских работ
ОК-8 способностью к самоорганизации и самообразованию;		Задание 1	Организация аналитической работы по предупреждению утечки конфиденциальной информации.
		Задание 2	Организация построения как отдельных процессов управления ИБ, так и системы процессов в целом.
Профессиональные компетенции (ПК):			
ПК-8 способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов;		Задание 1	Разработка проекта охранной сигнализации на примере 3-го этажа выставочного зала.
		Задание 2	Разработка проекта охранной сигнализации на примере складского помещения металлопроката.
ПК-9 способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;		Задание 1	Разработка проекта охранной сигнализации на примере одноэтажного отеля.
		Задание 2	Разработка проекта охранной сигнализации на примере 4-го этажа офисного зала.
ПК-12 способностью принимать участие в проведении экспериментальных исследований системы защиты информации		Задание 1	Разработка проекта охранной сигнализации на примере одноэтажного отеля.
		Задание 2	Разработка проекта охранной сигнализации на примере помещения магазина и кафе.
Профессиональные специальные компетенции (ПК):			
ПСК-1 способностью участвовать в разработке и эксплуатации подсистемы управления информационной безопасностью		Задание 1	Разработка проекта охранной сигнализации на примере складского помещения обувной продукции.
		Задание 2	Разработка проекта охранной сигнализации на примере

		производственного центра строительной продукции.
ПСК-2 способностью применять современные информационные технологии и методы цифровой обработки сигналов для эффективного анализа и использования массивов информации при решении задач обеспечения информационной безопасности автоматизированных систем	Задание 1	Разработка охранного комплекса на основе радиоканала.
	Задание 2	Разработка проекта охранной сигнализации на примере 2-го этажа выставочного зала.

Задания, позволяющие оценить умения и навыки, полученные на практике (повышенный уровень)

Контролируемые компетенции или их части		Формулировка задания	
Код компетенции	Формулировка		
Общекультурные компетенции (ОК):			
ОК-5 способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики;		Задание 1	Разработка проекта охранной сигнализации на примере подвального хранилища скобяных изделий.
		Задание 2	Разработка проекта охранной сигнализации на примере восьмикомнатного офиса
ОК-8 способностью к самоорганизации и самообразованию;		Задание 1	Разработка проекта охранной сигнализации на примере гаража на 20 автомобилей.
		Задание 2	Разработка проекта охранной сигнализации на примере автомастерской легковых автомобилей
Профессиональные компетенции (ПК):			
ПК-8 способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов;		Задание 1	Разработка проекта охранной сигнализации на примере магазина ювелирных изделий.
		Задание 2	Разработка проекта охранной сигнализации на примере автомастерской легковых автомобилей.
ПК-9 способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических		Задание 1	Разработка проекта охранной сигнализации на примере одноэтажного офиса.
		Задание 2	Разработка проекта охранной сигнализации на примере

материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;		производственного центра строительной продукции.
ПК-12 способностью принимать участие в проведении экспериментальных исследований системы защиты информации	Задание 1	Разработка проекта охранной сигнализации на примере рабочего литейного цеха.
	Задание 2	Разработка проекта охранной сигнализации на примере жилого 5-ти квартирного жилого дома.
Профессиональные специальные компетенции (ПК):		
ПСК-1 способностью участвовать в разработке и эксплуатации подсистемы управления информационной безопасностью	Задание 1	Разработка проекта охранной сигнализации на примере загородного жилого дома.
	Задание 2	Разработка проекта охранной сигнализации на примере магазина спортивных товаров.
ПСК-2 способностью применять современные информационные технологии и методы цифровой обработки сигналов для эффективного анализа и использования массивов информации при решении задач обеспечения информационной безопасности автоматизированных систем	Задание 1	Разработка проекта охранной сигнализации на примере административного здания.
	Задание 2	Разработка проекта охранной сигнализации на примере производственного корпуса предприятия легкой промышленности.

11.6. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

На каждом этапе практики осуществляется текущий контроль за процессом формирования компетенций. Предлагаемые обучающемуся задания позволяют проверить компетенции: ОК-5, ОК-8, ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-8, ПК-9, ПК-12, ПК-13, ПК-14, ПК-15ПСК-5, ПСК-6.

Задания предусматривают овладение компетенциями на разных уровнях: базовом и повышенном. Для продвинутого уровня, предусмотрены, задания повышенной сложности.

При организации и проведении производственной практики необходимо:

- на начальном этапе провести анализ предметной области по теме исследования, провести сбор и обработку материалов по теме исследования – 27 час.
- на промежуточном этапе разработать техническое задание по теме исследования – 27 час.
- на заключительном этапе провести анализ полученных результатов, формирование предложений по теме исследования - 27 час.

Структура отчета проведенных научных исследований: введение; аналитический обзор по теме исследования; разработка программ и методик проведения исследований; заключение; список использованных источников.

Рекомендуемые формы по оформлению материалов отчета представлены в приложениях к настоящим указаниям.

При проверке задания, оцениваются:

–грамотно составленный аналитический отчет;

–последовательность изложения материала;

–грамотная формулировка актуальности рассматриваемых выработанных предложений;

–постановка и решение проблемы по теме научного исследования.

При защите отчета оцениваются:

–знания современных средств, видов и методик систем информационной безопасности;

–знания технологии умение их при решении практических задач при решении практических задач;

–выводы и предложения по результатам выполненной работы.

–

12. Методические рекомендации для обучающихся по прохождению практики

На первом этапе необходимо ознакомиться со структурой практики, обязательными видами работ и формами отчетности, которые отражены в Методических указаниях по практике.

Для успешного выполнения заданий по преддипломной практике, обучающемуся необходимо самостоятельно детально изучить представленные источники литературы

№ п/п	Вид самостоятельной работы	Рекомендуемые источники информации (№ источника)			
		Основная	Дополнительная	Методическая	Интернет-ресурсы
1	Сбор материалов по структуре предприятия, правил документооборота	1,2	1,2	1	1,2
2	Подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по инженерно-технической защите объектов информатизации, современным аппаратным и программным средствам защиты информации, а так же подбор материала в соответствии с выбранной тематикой дипломного проектирования.	1,2	1,2	1	1,2
3	проведение экспериментов по заданной методике, обработка и анализ результатов.	1,2	1,2	1	1,2
4	сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ	1,2	1,2	1	1,2

	подсистем по показателям информационной безопасности.				
5	совершенствование системы управления информационной безопасностью.	1,2	1,2	1	1,2
7	Оформление отчёта по практике.	1,2	1,2	1	1,2

13. Учебно-методическое, информационное и материально-техническое обеспечение практики

13.1. Перечень учебной литературы и ресурсов сети «Интернет», необходимых для проведения практики

13.1.1. Перечень основной литературы:

1. Чернышев, А. Б. (Институт сервиса, туризма и дизайна (филиал)СКФУ в г. Пятигорске). Теория информационных процессов и систем : учеб. пособие / А.Б. Чернышев, В.Ф. Антонов, Г.Б. Суюнова ; Сев.-Кав. федер. ун-т. - Ставрополь : СКФУ, 2015. - 169 с..
2. Кочетков М.В. Системы охраны [Электронный ресурс]: учебное пособие/ Кочетков М.В.— Электрон. текстовые данные.— Саратов: Вузовское образование, 2015.— 99 c.— Режим доступа: http://www.iprbookshop.ru/29284.— ЭБС «IPRbooks», по паролю.

13.1.2. Перечень дополнительной литературы

1. Шаньгин В.Ф.Комплексная защита информации в корпоративных системах: учебное пособие. – М.: ИНФРА-М, 2012.
2. Федотов Е.А. Администрирование программных и информационных систем [Электронный ресурс]: учебное пособие/ Федотов Е.А.— Электрон. текстовые данные.— Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, ЭБС АСВ, 2012.— 136 c.— Режим доступа: http://www.iprbookshop.ru/27280.— ЭБС «IPRbooks», по паролю.

13.1.3. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по практике:

1. Методические указания по организации и проведению эксплуатационной практики для студентов, обучающихся по направлению подготовки 10.03.01 «Информационная безопасность».

13.1.4. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. http://elibrary.ru - Научная электронная библиотека eLIBRARY.RU
2. http://www.biblioclub.ru -Университетская библиотека online

14. Перечень информационных технологий, используемых при проведении практики, включая перечень программного обеспечения и информационных справочных систем Информационные технологии:

- Мультимедийные технологии: проекторы, ноутбуки, персональные компьютеры, комплекты презентаций, учебные фильмы.
- Дистанционная форма консультаций во время прохождения конкретных этапов практики и подготовки отчета, которая обеспечивается: выходом в глобальную сеть Интернет, поисковыми системами Яндекс, Мейл, Гугл, системами электронной почты.
- Компьютерные технологии и программные продукты: Электронная-библиотечная система (ЭБС) IPRboks.ru; Наличие базы данных электронного каталога – Фолиант.
- Пакет программ MicrosoftOffice;
- MathCAD;
- MathLAB.

Информационные справочные системы:

- Компьютерная справочно-правовая система «Гарант».
- Электронная информационно-образовательная среда Е-кампус.

Перечень программного обеспечения и информационных справочных систем

–Microsoft Office – 61541869, Microsoft Windows 7 Профессиональная -61541869

–1С: Предприятие 8. Комплект для обучения в высших и средних учебных заведениях (рег. номер 9334708), AutoCAD 2015 (бесплатный для вузов), Embarcadero rad studio - Г/к 445/01 от 30 июля 2010 г., IBM Rational Rose modeler (бесплатно по программе IBM Academic Initiative), Mathcad Education - University Edition (50 pack) -договор № 24-эа/15 от 19 августа 2015г., Microsoft Office - №61541869, Cisco Packet Tracer - договор № 23-с от 27 июня 2012 г., Microsoft Windows 7 Профессиональная - №61541869, Visual Studio IDE – AzureDev ID: a6c2b0d7-162e-479f-8a58-384701f33665, Microsoft Visual Basic – AzureDev ID: a6c2b0d7-162e-479f-8a58-384701f33665, Microsoft SQL Server – AzureDev ID: a6c2b0d7-162e-479f-8a58-384701f33665, PascalABC.NET (бесплатный), Oracle VM VirtualBox (бесплатный).

15. Описание материально-технической базы, необходимой для проведения практики

Определяется структурой места прохождения практики, если практика проходит на кафедре ВУЗа используется следующее материально-техническое обеспечение:

- переносной проектор Acer PO100 экран LUMA 1300, ноутбук (1 шт) Asus K50I T44002.2/3072/GT320M/250/5400/DVD-RW, наборы демонстрационного оборудования и учебно-наглядных пособий.
- специализированная учебная мебель и технические средства обучения, служащие для представления учебной информации: компьютеры (5 шт) с подключением к сети "Интернет" и доступом в электронную информационно-образовательную среду, книжные шкафы для учебной литературы и учебно-методических материалов