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

ПРЕДДИПЛОМНАЯ 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.

Профессор кафедры систем управления и информационных технологий
_____ А.Б.Чернышев
«__» _____ 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
«__» _____ 2020 г.

ПРОГРАММА ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

ПРЕДДИПЛОМНАЯ 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 СУиИТ
_____ И.М.Першин
«__» _____ 201_ 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.

Профессор кафедры систем управления и информационных технологий
_____ А.Б.Чернышев
«__» _____ 2020 г.

Пятигорск, 2020

1. **Цели практики**

Целями преддипломной практики по направлению подготовки 10.03.01 Информационная безопасность являются:

1) закрепление, расширение, углубление и систематизация знаний, полученных при изучении специальных дисциплин;
2) приобретение практических навыков и компетенций в сфере профессиональной деятельности;
3) подбор необходимого материала для выполнения дипломного проектирования.

2. **Задачи практики**:

Задачами преддипломной 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, в том числе сравнительного анализа типовых криптосхем. 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

Преддипломная практика относится к блоку 2 «Практики», ее освоение происходит в 8-м семестре. Практика базируется на следующих дисциплинах: «Основы информационной безопасности», «Методы проектирования систем технической охраны объектов информатизации», «Эксплуатационная 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 должны быть использованы в дальнейшем в подготовке выпускных квалификационных работ.

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

- вид практики – производственная;
- тип практики – преддипломная;
- способ проведения практики - стационарный;
- форма проведения практики - непрерывно.

5. Место и время проведения практики

Преддипломная практика проводится на 4 курсе в 8 семестре в течение 6 недель на основании учебного плана для данного направления подготовки.

Преддипломная практика может проводиться в структурных подразделениях организаций (предприятий и фирм) различных формсобственности на основе прямых договоров, заключаемых между организациейи университетом. При наличии вакантных должностей студенты могутзачисляться на них, если работа соответствует требованиям программыпрактики.

Рабочие места для студентов могут выделяться в структурных подразделениях, связанных с исследованиями, проектированием, организацией и эксплуатацией информационных систем и систем защиты информации. К таким подразделениям относятся:

1) научно-исследовательские отделы;
2) конструкторские отделы;
3) технологические отделы;
4) отделы испытаний;
5) отделы и лаборатории, занимающиеся автоматизацией проектирования и управления производством;
6) службы АСУ;
7) службы режима работы предприятия.

В этих подразделениях студенты-практиканты могут выполнять функции разработчика, исследователя, программиста и т.п.

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
ПСК-5	способностью разработать комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации, провести выбор необходимых технологий и технических средств, организовать его внедрение и последующее сопровождение

ПСК-6	способностью формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности

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	Знакомство с коллективом организации, с его деятельностью и нормативными документами	Владеть методикой проверки защищенности объектов информатизации на соответствие требованиям нормативных документов	Обобщать научно-техническую литературу, нормативно-методические материалы по инженерно-технической защите информации	Знать вопросы нормирования, организации и оплаты труда, вопросы обеспечения безопасности жизнедеятельности на предприятии
ОК-8	Самостоятельное знакомство и анализнормативных документов, связанных с защитой информации на данном предприятии	Владеть методикой исследования защищенности объектов информатизации от утечки информации	Подбирать, научно-техническую литературу по инженерно-технической защите информации	Знать основные правовые положения в области информационной безопасности и защиты информации
ПК-8	Знакомство с локальными документами, связанными с защитой информации на данном предприятии	Владеть методикой изучения локальных документов защищенности объектов от утечки информации на предмет их соответствия нормативной документации	Оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	Знать рабочую техническую документацию с учетом действующих нормативных и методических документов
ПК-1	способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Владеть работами по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Оформлять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Знать 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,	владеть способностью применять программные средства	применять программные средства системного, прикладного и специального	знать программные средства системного, прикладного и специального назначения,

	прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	инструментальные средства, языки и системы программирования для решения профессиональных задач
ПК-3	способностью администрировать подсистемы информационной безопасности объекта защиты	владеть способностью администрировать подсистемы информационной безопасности объекта защиты	администрировать подсистемы информационной безопасности объекта защиты	знать 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	участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	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	принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации
ПК-9	Составление краткого отчета об уровне защищенности данного предприятия от утечки информации	Владеть методами составления обзора по вопросам обеспечения информационной безопасности	Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, по профилю своей профессиональной деятельности	Знать методы и приемы подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов по профилю своей профессиональной деятельности
ПК-12	Проведение анкетирования работников организации с целью исследования системы защиты информации	Владеть навыками обработки экспериментальных данных	Уметь проводить экспериментальные исследования системы защиты информации	Знать методы и приемы проведения 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	принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	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	организовывать работу малого коллектива исполнителей в профессиональной деятельности	организовывать работу малого коллектива исполнителей в профессиональной деятельности	знать и 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	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	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	знать и 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	Разработка подсистемы управления информационной безопасностью для отдельной структуры организации	Владеть технологией проектирования систем защиты информации	Участвовать в разработке подсистемы управления информационной безопасностью	Знать принципы организации информационных систем в соответствии с требованиями информационной защищенности
ПСК-2	Проанализировать результаты контрольных проверок, изучить и обобщить опыт эксплуатации объекта информатизации	Владеть приемамиобработки результатов анализа документации	Уметь применять современные информационные технологии и методы цифровой обработки сигналов для эффективного анализа обеспечения информационной безопасности автоматизированных	Знать современные информационные технологии и методы цифровой обработки сигналов для эффективного анализа обеспечения информационной безопасности автоматизированных систем

			систем	
ПСК-5	способностью разработать комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации, провести выбор необходимых технологий и технических средств, организовать его внедрение и последующее сопровождение	владеть комплексом организационных и технических мер по обеспечению информационной безопасности объекта информатизации, провести выбор необходимых технологий и технических средств, организовать его внедрение и последующее сопровождение	разработать комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации, провести выбор необходимых технологий и технических средств, организовать его внедрение и последующее сопровождение	знать и разработать комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации, провести выбор необходимых технологий и технических средств, организовать его внедрение и последующее сопровождение
ПСК-6	способностью формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности	владеть формированием комплексом мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности	формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности	Знать и формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности

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 профес-сиональной 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	ПК-1, ПК-2

эксплуатационная;	администрирование подсистем информационной безопасности объекта;	Проведение работ по установке и техническому обслуживанию защищенных технических средств обработки информации	организовать внедрение комплекса мер по организации информационной безопасности и его последующее сопровождение	ПК-3
	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	ПК-3, ПК-4
проектно-технологическая	сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;	Проектирование объектов в защищенном исполнении	составление краткого отчета об уровне защищенности данного предприятия от утечки информации	ПК-9, ПК-12
	проведение проектных расчетов элементов систем обеспечения информационной безопасности;	Проектирование объектов в защищенном исполнении	изучить и обобщить опыт эксплуатации объекта информатизации	ПСК-2
	участие в разработке технологической и эксплуатационной документации;	Проектирование объектов в защищенном исполнении	разработка подсистемы управления информационной безопасностью для отдельной структуры организации	ПСК-1
	проведение предварительного технико-экономического обоснования проектных расчетов;	Проектирование объектов в защищенном исполнении	утвердить сформированный комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности с руководством организации	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	ПК-12
	проведение вычислительных экспериментов с использованием стандартных программных средств;	Проведение сертификационных испытаний средств защиты информации на соответствие требованиям по безопасности информации	обработка экспериментальных данных, полученных при анкетировании	ПК-12
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	ПК-8
	контроль эффективности реализации политики	Проведение аттестации объектов на	изучение современных аппаратных и	ПСК-6

	информационной безопасности объекта защиты.	соответствие требованиям по защите информации	программных средства вычислительной техники	

7. Объем практики

Объем занятий: Итого 243 ч. 9 з.е.

Продолжительность 6 недель

Зачет с оценкой 8 семестр

8. Структура и содержание практики

Разделы (этапы) практики	Реализуемые компетенции	Виды работ обучающегося на практике	Кол-во часов	Формы текущего контроля
Производственный инструктаж	ОК-5	Инструктажи по технике безопасности и пожарной безопасности	12	
Изучение структуры предприятия, правил документооборота	ОК-8	Сбор, обработка и систематизация фактического материала	33	
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.	ПК 1, ПК 2, ПК 3, ПК 4, ПК 5, ПК-8, ПК-9	Сбор, обработка и систематизация фактического и литературного материала	33	
Экспериментально-исследовательская деятельность: проведение экспериментов по заданной методике, обработка и анализ результатов.	ПСК-1, ПСК-2	Наблюдения, измерения	33	
Проектная деятельность: сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности.	ПК-12, ПК 13, ПК 14, ПК 15	Сбор, обработка и систематизация фактического и литературного материала	33	
Организационно-управленческая деятельность: совершенствование	ПСК-1, ПСК-2	Самостоятельная работа	33	

системы управления информационной безопасностью.				
Эксплуатационная деятельность: администрирование подсистем информационной безопасности объекта.	ПСК-5	Самостоятельная работа	33	
Оформление отчёта по практике и его защита.	ПСК-6	Самостоятельная работа	33	Отчет по практике, зачет с оценкой

9. Формы отчетности по практике

1. Дневник

2. Отчет обучающегося

3. Отзыв руководителя практики от вуза

4. Отзыв руководителя практики от профильной организации

Структура отчета по практике:

1. Содержание
2. Задания
3. Основная часть
4. Индивидуальное задание
5. Заключение
6. Список использованных источников
7. Приложения

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	Инструктажи по технике безопасности и пожарной безопасности	Производственный инструктаж	Отчет	11	1	12
ОК-8	Сбор материалов по структуре предприятия, правил документооборота	Индивидуальное задание	Отчет	32,5	0,5	33
ПК 1, ПК 2, ПК 3, ПК 4,	Подбор, изучение и обобщение научно-технической литературы, нормативных и	Индивидуальное задание	Отчет	32,5	0,5	33

ПК 5, ПК-8, ПК-9	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.					
ПСК-1, ПСК-2	Экспериментально-исследовательская деятельность: проведение экспериментов по заданной методике, обработка и анализ результатов.	Индивидуальное задание	Отчет	32,5	0,5	33
ПК-12, ПК 13, ПК 14, ПК 15	Проектная деятельность: сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности.	Индивидуальное задание	Отчет	32,5	0,5	33
ПСК-1, ПСК-2	Организационно-управленческая деятельность: совершенствование системы управления информационной безопасностью.	Индивидуальное задание	Отчет	32,5	0,5	33
ПСК-5	Эксплуатационная деятельность: администрирование подсистем информационной безопасности объекта.	Индивидуальное задание	Отчет	32,5	0,5	33
ПСК-6	Оформление отчёта по практике.	Индивидуальное задание	Публичная защита выполненной работы, по итогам которой выставляется зачет с оценкой	33		33
			Итого за 8 семестр	**239**	**4**	**243**

Итого	**239**	**4**	**243**

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

Фонды оценочных средств, позволяющие оценить уровень сформированностикомпетенций, размещен в УМК преддипломной практики на кафедре СУиИТ 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-9,	Начальный	собеседование	текущий	текущий	Задания для проверки уровня знаний
ПК 1, ПК 2, ПК 3, ПК 4, ПК 5, ПК-8, ПК-9, ПК-12, ПСК-1, ПСК-2, ПСК-5, ПСК-6	Промежуточный	Собеседование	текущий	текущий	Задания для проверки уровня умений и навыков
ПК 1, ПК 2, ПК 3, ПК 4, ПК 5, ПК-8, ПК-9, ПК-12, ПСК-1, ПСК-2, ПСК-5, ПСК-6	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 компетенций	Индикаторы	Дескрипторы			
		2 балла	3 балла	4 балла	5 баллов*
Базовый	Знание: современные аппаратные и программные средства вычислительной техники;	Отсутствует знания: современных аппаратных и программных средств	Имеются знания: современных аппаратных и программных средств	Знает: современные аппаратные и программные средства вычислительной	

	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;	вычислительной техники; принципов организации информационных систем в соответствии с требованиями информационной защищенности и в соответствии с требованиями по защите государственной тайны; - конструкции и основных характеристик технических устройств хранения, обработки и передачи информации; - 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;	вычислительной техники; принципов организации информационных систем в соответствии с требованиями информационной защищенности и в соответствии с требованиями по защите государственной тайны; - конструкции и основных характеристик технических устройств хранения, обработки и передачи информации; - 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;	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;	
	Умение: подбирать, обобщать научно-техническую литературу, нормативно-методические материалы по инженерно-технической защите информации; внедрять комплексные	Отсутствует умения: подбирать, обобщать научно-техническую литературу, нормативно-методические материалы по	Имеются умения: подбирать, обобщать научно-техническую литературу, нормативно-методические материалы по	Умеет: подбирать, обобщать научно-техническую литературу, нормативно-методические материалы по инженерно-	

	системы и отдельные специальные технические и программно-математические средства защиты информации на объектах информатизации, в том числе сравнительного анализа типовых криптосхем;	инженерно-технической защите информации; внедрять комплексные системы и отдельные специальные технические и программно-математические средства защиты информации на объектах информатизации, в том числе сравнительного анализа типовых криптосхем;	инженерно-технической защите информации; внедрять комплексные системы и отдельные специальные технические и программно-математические средства защиты информации на объектах информатизации, в том числе сравнительного анализа типовых криптосхем;	технической защите информации; внедрять комплексные системы и отдельные специальные технические и программно-математические средства защиты информации на объектах информатизации, в том числе сравнительного анализа типовых криптосхем;	
	Владение: 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 проектирования, построения и эксплуатации комплексных систем защиты информации	Имеются навыки владения: методами организации и управления деятельностью служб защиты информации на предприятии; технологией проектирования, построения и эксплуатации комплексных систем защиты информации	Владеет: методами организации и управления деятельностью служб защиты информации на предприятии; технологией проектирования, построения и эксплуатации комплексных систем защиты информации;	
Повышенный	Знание 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; вопросы нормирования, организации и оплаты				Знает: принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; принципы построения современных криптографических систем, стандарты в области

	труда, вопросы обеспечения безопасности жизнедеятельности на предприятии.				криптографической защиты информации; основные правовые положения в области информационной безопасности и защиты информации; вопросы нормирования, организации и оплаты труда, вопросы обеспечения безопасности жизнедеятельности на предприятии.
	Умение: разрабатывать предложения по совершенствованию и повышению эффективности применяемых мер на основе анализа результатов контрольных проверок, изучения и обобщения опыта эксплуатации объекта информатизации.				Умеет: разрабатывать предложения по совершенствованию и повышению эффективности применяемых мер на основе анализа результатов контрольных проверок, изучения и обобщения опыта эксплуатации объекта информатизации.
	Владение: 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 безопасностиимеются, 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 методических документов;	Задание 1	Изучение технической документации.
	Задание 2	Изучение методических документов по защите информации.
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	Изучение современных разработок по технической защите информации.
	Задание 2	Изучение технической защиты информации на предприятии.
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	Изучение документации по защите информации на конкретном предприятии.
	Задание 2	Изучение российской нормативной документации по защите информации.
ПСК-3 способностью изучать и обобщать опыт работы различных учреждений, организаций и предприятий в области повышения эффективности защиты информации	Задание 1	Изучение современных разработок по технической защите информации.
	Задание 2	Изучение технической защиты информации на предприятии.
ПК-4 способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Задание 1	Сбор материалов по структуре предприятия.
	Задание 2	Изучение правил документооборота на предприятии.
ПК-5 способностью участвовать в работах по реализации политики информационной безопасности,	Задание 1	Обзор технических средств и необходимых для их установки технологий.
	Задание 2	Изучение правил внедрения и адаптации систем

применять комплексный подход к обеспечению информационной безопасности объекта защиты		безопасности.
ПСК-6 способностью формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности.	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):			
		Задание 1	Изучение рекомендаций по технике безопасности при проведении работ по установке технических средств защиты информации.
		Задание 2	Изучение характеристик аппаратных средств и программного обеспечения.
ОК-8 способностью к самоорганизации и самообразованию;		Задание 1	Изучение программного и технического обеспечения защиты информации на предприятии.
		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-1способностью участвовать в разработке и эксплуатации подсистемы управления информационной безопасностью		Задание 1	Изучение технической защиты информации на различных предприятиях.
		Задание 2	Разработка предложений по техническому обеспечению защиты информации.
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	Изучение российской нормативной и правовой документации по защите информации.
		Задание 2	Изучение международной нормативной документации по защите информации.
ПСК-1способностью участвовать в		Задание 1	Изучение технических средств защиты

разработке и эксплуатации подсистемы управления информационной безопасностью		информации на предприятии и их основных характеристик.
	Задание 2	Разработка предложений по техническому обеспечению защиты информации.
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	Изучение правил документооборота на предприятии с учетом его защищенности при передаче по сетям.
	Задание 2	Изучение системы защиты информации на предприятии.
ПСК-5 способностью разработать комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации, провести выбор необходимых технологий и технических средств, организовать его внедрение и последующее сопровождение	Задание 1	Изучение правил внедрения и адаптации современных систем безопасности.
	Задание 2	Изучение методов тестирования компонентов информационных систем.
ПСК-6 способностью формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности.	Задание 1	Изучение правил настройки современных систем безопасности.
	Задание 2	Изучение методов инсталляции программного обеспечения информационных систем.

Задания, позволяющие оценить умения и навыки, полученные на практике (базовый 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	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 технической документации.
		Задание 2	Разработка методических документов по защите информации.
ПК-9 способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных		Задание 1	Решение стандартных задач профессиональной деятельности на основе информационной и библиографической культуры.

и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;	Задание 2	Владение навыками применения информационно-коммуникационных технологий.
ПК-12 способностью принимать участие в проведении экспериментальных исследований системы защиты информации	Задание 1	Применение механизмов использования аппаратных средств и программного обеспечения.
	Задание 2	Применение процедур и результатов использования аппаратных средств и программного обеспечения.
Профессиональные специальные компетенции (ПК):		
ПСК-1 способностью участвовать в разработке и эксплуатации подсистемы управления информационной безопасностью	Задание 1	Применение современных разработок по технической защите информации.
	Задание 2	Разработка системы технической защиты информации на предприятии.
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	Проектирование систем безопасности на предприятии.
	Задание 2	Внедрение и сопровождение систем безопасности на предприятии.
ПСК-1способностью участвовать в разработке и эксплуатации подсистемы управления информационной безопасностью	Задание 1	Использование нормативно-правовых документов в процессе эксплуатации систем защиты информации.
	Задание 2	Анализ и моделирование процессов в системах защиты информации.
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	Использование современных информационно-коммуникационных технологий при решении профессиональных задач защиты информации.
	Задание 2	Использование различных способов обеспечения информационной безопасности.
ПСК-5 способностью разработать комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации, провести выбор необходимых технологий и технических средств, организовать его внедрение и последующее сопровождение	Задание 1	Внедрение на практике технических средств по защите информации при помощи необходимых для их установки технологий.
	Задание 2	Сопровождение на практике технических средств по защите информации.
ПСК-6 способностью формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности.	Задание 1	Экономическая обоснованность предлагаемых средств защиты информации.
	Задание 2	Расчет экономической целесообразности предлагаемых средств защиты информации.

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

Контролируемые компетенции или их части		Формулировка задания
Код	Формулировка	

компетенции		
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 профилактической работы с персоналом организации по предупреждению утечки конфиденциальной информации.
	Задание 2	Составление рекомендаций по технике безопасности при проведении проектно-конструкторских работ и ознакомление с ними персонала организации.
ОК-8 способностью к самоорганизации и самообразованию;	Задание 1	Составление различных диаграмм и графиков, освещающих ситуацию с защитой информации на предприятии.
	Задание 2	Написание тезисов для выступления на конференции по итогам практики.
Профессиональные компетенции (ПК):		
ПК-8 способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов;	Задание 1	Разработка технической документации на основании существующих в организации документов.
	Задание 2	Разработка методических документов по защите информации и доведение их до сведения персонала организации.
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	Решение усложненных задач профессиональной деятельности на основе информационной и библиографической культуры.
	Задание 2	Владение навыками применения информационно-коммуникационных технологий в конкретных ситуациях.
ПК-12 способностью принимать участие в проведении экспериментальных исследований системы защиты информации	Задание 1	Уверенное применение механизмов использования аппаратных средств и программного обеспечения.
	Задание 2	Уверенное применение процедур и результатов использования аппаратных средств и программного обеспечения.
Профессиональные специальные компетенции (ПК):		
ПСК-1 способностью участвовать в разработке и эксплуатации подсистемы управления информационной безопасностью	Задание 1	Введение в эксплуатацию современных разработок по технической защите информации.
	Задание 2	Введение в эксплуатацию системы технической защиты информации на предприятии.
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	Введение в эксплуатацию систем безопасности на предприятии.
	Задание 2	Профессиональное сопровождение систем безопасности на предприятии.
ПСК-1способностью участвовать в разработке и эксплуатации подсистемы управления информационной безопасностью	Задание 1	Использование не только российских, но и международных нормативно-правовых документов в процессе эксплуатации систем защиты информации.
	Задание 2	Анализ и моделирование процессов в системах защиты информации с использованием не только российских, но и зарубежных разработок.
ПСК-2 способностью применять современные информационные технологии и методы цифровой	Задание 1	Уверенное применение современных информационно-коммуникационных технологий при решении профессиональных задач защиты

обработки сигналов для эффективного анализа и использования массивов информации при решении задач обеспечения информационной безопасности автоматизированных систем		информации.
	Задание 2	Уверенное применение различных способов обеспечения информационной безопасности.
ПСК-5 способностью разработать комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации, провести выбор необходимых технологий и технических средств, организовать его внедрение и последующее сопровождение	Задание 1	Уверенное применение на практике технических средств по защите информации при помощи необходимых для их установки технологий.
	Задание 2	Умение тестировать компоненты систем защиты информации при помощи различных методик.
ПСК-6 способностью формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности.	Задание 1	Уверенное применение экономической обоснованности предлагаемых средств защиты информации.
	Задание 2	Расчет экономической целесообразности и окупаемости предлагаемых средств защиты информации.

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-15, ПСК-1, ПСК-2, ПСК-5, ПСК-6.

Задания предусматривают овладение компетенциями на разных уровнях: базовом и повышенном.Их принципиальное отличие в уровне овладения знаниями, умениями и навыками, классифицированные выше.

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	Экспериментально-исследовательская деятельность: проведение экспериментов по заданной методике, обработка и анализ результатов.	1,2	1,2	1	1,2
4	Проектная деятельность: сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности.	1,2	1,2	1	1,2
5	Организационно-управленческая деятельность: совершенствование системы управления информационной безопасностью.	1,2	1,2	1	1,2
6	Эксплуатационная деятельность: администрирование подсистем информационной безопасности объекта.	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. Галатенко В.А. Основы информационной безопасности [Электронный ресурс]/ Галатенко В.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 266 с.— Режим доступа: http://www.iprbookshop.ru/52209.— ЭБС «IPRbooks», по паролю
2. Методы проектирования систем технической охраны объектов : лабораторный практикум / сост. И.В. Калиберда ; Сев.-Кав. федер. ун-т. - Ставрополь : СКФУ, 2015. - 129 с. - Библиогр. в конце глав

13.1.2. Перечень дополнительной литературы

3. Фаронов А.Е. Основы информационной безопасности при работе на компьютере [Электронный ресурс]/ Фаронов А.Е.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 154 с.— Режим доступа: http://www.iprbookshop.ru/52160.— ЭБС «IPRbooks», по паролю.
4. Методы проектирования систем технической охраны объектов : учеб. пособие / П.П. Мулкиджанян, Ю.Г. Айвазов, В.В. Родишевский и др. ; Сев.-Кав. федер. ун-т. - Ставрополь : СКФУ, 2015. - 163 с. - Прил.: с. 83-159. - Библиогр.: с. 82

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

1. Методические указания по организации и проведению преддипломной 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.

Информационные справочные системы:

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

Перечень программного обеспечения и информационных справочных систем

–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: 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.