

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

УТВЕРЖДАЮ
Директор Пятигорского института
(филиал) СКФУ
Т.А. Шебзухова
«__» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ПРАКТИКИ
Преддипломная практика

(ЭЛЕКТРОННЫЙ ДОКУМЕНТ)

Направление подготовки/специальность 10.03.01 Информационная безопасность
Квалификация выпускника: бакалавр
Форма обучения очная
Год начала обучения 2021
Изучается в **8** семестре

Пятигорск, 2021 г.

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 форм собственности на основе прямых договоров, заключаемых между организацией и университетом. При наличии вакантных должностей студенты могут зачисляться на них, если работа соответствует требованиям программы практики.

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:
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-6	Способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации
ПК-7	Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений
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-10	Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности
ПК-11	Способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов
ПК-12	способностью принимать участие в проведении экспериментальных исследований системы защиты информации

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
ПК-1	способностью выполнять работы	Владеть работами по установке,	Оформлять работы по установке,	Знать работы по установке, настройке и

	по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	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	владеть способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	знать 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	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-6	Способность принимать участие в организации и проведении	принимать участие в организации и проведении контрольных	принимать участие в организации и проведении контрольных	участие в организации и проведении контрольных проверок работоспособности и

	контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	эффективности применяемых программных, программно-аппаратных и технических средств защиты информации
ПК-7	Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений
ПК-8	Способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	рабочую техническую документацию с учетом действующих нормативных и методических документов
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-10	Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности

ПК-11	Способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов
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

6.3. Соответствие планируемых результатов видам профессиональной деятельности

Планируемые результаты сформулированы в соответствии с профессиональным стандартом «Специалист по технической защите информации»

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)
эксплуатационная;	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
	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	Проведение аттестации объектов на соответствие требованиям по защите информации	внедрять комплексные системы и отдельные специальные и программно-математические средства защиты	ПК-3, ПК-4

	систем;		информации на объектах информатизации	
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
	участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	изучить и обобщить опыт эксплуатации объекта информатизации	ПК-6
	участие в разработке технологической и эксплуатационной документации;	Проектирование объектов в защищенном исполнении	разработка подсистемы управления информационной безопасностью для отдельной структуры организации	ПК-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-11
	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	организация внедрения и последующего	ПСК-5

организационно-управленческая.		технической защите информации	сопровождение разработанного проекта	
	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	ПК-7
	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 информационной безопасности объекта защиты.	Проведение аттестации объектов на соответствие требованиям по защите информации	изучение современных аппаратных и программных средства вычислительной техники	ПК-10

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	ПК-1, ПК-2	Инструктажи по технике безопасности и пожарной безопасности	12	
Изучение структуры предприятия, правил документооборота	ПК-12, ПК-11, ПК-10	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.	ПК-1, ПК-2, ПК-8	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	Сбор, обработка и систематизация фактического и литературного материала	33	
Организационно-управленческая деятельность: совершенствование системы управления информационной безопасностью.	ПК-1, ПК-2	Самостоятельная работа	33	
Эксплуатационная деятельность: администрирование подсистем информационной безопасности объекта.	ПК-5	Самостоятельная работа	33	
Оформление отчёта по практике и его защита.	ПК-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 реализованных компетенций	Вид деятельности обучающегося	Итоговый продукт самостоятельной работы	Средства и технологии оценки	Объем часов, в том числе		
				СРС	Контактная работа с преподавателем	Всего
ПК-5	Инструктажи по технике безопасности и пожарной безопасности	Производственный инструктаж	Отчет	11	1	12
ПК-8	Сбор материалов по структуре предприятия, правил документооборота	Индивидуальное задание	Отчет	32,5	0,5	33
ПК 3, ПК 4, ПК 5, ПК-6, ПК-8, ПК-7	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 также подбор материала в соответствии с выбранной тематикой дипломного проектирования.	Индивидуальное задание	Отчет	32,5	0,5	33
ПК-1, ПК-2	Экспериментально-исследовательская деятельность: проведение экспериментов по заданной методике, обработка и анализ результатов.	Индивидуальное задание	Отчет	32,5	0,5	33
ПК-10	Проектная деятельность: сбор и анализ исходных данных для проектирования систем защиты информации,	Индивидуальное задание	Отчет	32,5	0,5	33

	определение требований, сравнительный анализ подсистем по показателям информационной безопасности.					
ПК-11	Организационно-управленческая деятельность: совершенствование системы управления информационной безопасностью.	Индивидуальное задание	Отчет	32,5	0,5	33
ПК-12,	Эксплуатационная деятельность: администрирование подсистем информационной безопасности объекта.	Индивидуальное задание	Отчет	32,5	0,5	33
ПК-9	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 сформированности компетенций, 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
ПК 1, ПК 2, ПК 3	Начальный	собеседование	текущий	текущий	Задания для проверки уровня знаний

ПК 4, ПК 5, ПК-6, ПК-8, ПК-7	Промежуточн ый	Собеседован ие	текущий	текущий	Задания для проверки уровня умений и навыков
ПК-9, ПК- 10, ПК-11, ПК-12	Заключительн ый	Защита отчета	промежуточн ый	промежуточн ый	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; 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;	Отсутствует знания: современных аппаратных и программных средств 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	Имеются знания: современных аппаратных и программных средств 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	Знает: 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,	

		и характеристик аппаратуры, используемой для перехвата и анализа сигналов в технических каналах утечки информации; - методов и средств инженерно-технической защиты информации;	и характеристик аппаратуры, используемой для перехвата и анализа сигналов в технических каналах утечки информации; - методов и средств инженерно-технической защиты информации;	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 системы и отдельные специальные технические и программно-математические средства защиты информации на объектах информатизации, в том числе сравнительного анализа типовых криптосхем;	Отсутствует умения: 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, в том числе сравнительного анализа типовых криптосхем;	Имеются умения: 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, в том числе сравнительного анализа типовых криптосхем;	Умеет: 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, 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	Имеются навыки владения: методами организации и управления деятельностью служб защиты информации на предприятии; технологией проектирования, построения и эксплуатации	Владеет: методами организации и управления деятельностью служб защиты информации на предприятии; технологией проектирования, построения и эксплуатации комплексных систем защиты	

		комплексных систем защиты информации	комплексных систем защиты информации	информации;	
Повышенный	<p>Знание принципов и методов 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 труда, вопросы обеспечения безопасности жизнедеятельности на предприятии.</p>				<p>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; вопросы нормирования, организации и оплаты труда, вопросы обеспечения безопасности жизнедеятельности на предприятии.</p>
	<p>Умение: разрабатывать предложения по совершенствованию и повышению эффективности применяемых мер на основе анализа результатов контрольных проверок, изучения и обобщения опыта эксплуатации объекта</p>				<p>Умеет: разрабатывать предложения по совершенствованию и повышению эффективности применяемых мер на основе анализа результатов контрольных</p>

	информатизации.				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 безопасности и 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 безопасности в 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 безопасности имеются, 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 (ПСК):		
ПСК-1 способностью участвовать в разработке и эксплуатации подсистемы управления информационной	Задание 1	Изучение современных разработок по технической защите информации.
	Задание 2	Изучение технической защиты информации на

безопасностью		предприятию.
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, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Задание 1	Обзор технических средств и необходимых для их установки технологий.
	Задание 2	Изучение правил внедрения и адаптации систем 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.

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

Контролируемые компетенции или их части		Формулировка задания	
Код компетенции	Формулировка		
Профессиональные компетенции (ПК):			
ПК-8 способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов;	Задание 1	Изучение методов тестирования компонентов систем по 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.	

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

Контролируемые компетенции или их части		Формулировка задания	
Код компетенции	Формулировка		
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 и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;		Задание 1	Решение стандартных задач профессиональной деятельности на основе информационной и библиографической культуры.
		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.

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	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,		Задание 1	Решение усложненных задач профессиональной деятельности на основе информационной и библиографической культуры.
		Задание 2	Владение навыками применения информационно-

составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;		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.

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: ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6, ПК-7, ПК-8, ПК-9, ПК-10, ПК-11, ПК-12. 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	1,2	1,2	1	1,2

	соответствии с выбранной тематикой дипломного проектирования.				
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), 2018.— 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, 2019. - 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), 2017.— 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, 2017. - 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) IPRbooks.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.