Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Таныгин Максим Олегович

ФИО: Таныгин Максим Олегович Должность: и.о. декана факультета фундаментальной и прикладной информатики РОССИИ

Дата подписания: 21.02.2024 13:12:10

Уникальный программный ключ:

Юго-Западный государственный университет

65ab2aa0d384efe8480e6a4c688eddbc475e411a

УТВЕРЖДАЮ:	
Декан факультета	a
(наименование ф-та, полност	ью)
фундаментальной	і́ и прикладной
информатики	
подпась, инициалы, фамилия)	_ Таныгин М.О
(3/» Of	2021 г.

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

Производственная преддипломная практика (наименование вида и типа практики)

011011 во 10.05.02 информационная оезопасность			
	шифр и наименование направление подготовки (специальности)		
-11-1	телекоммуникационных систем		
Управл	ение безопасностью телекоммуникационных систем и сетей		
	наименование направленности (профиля, специализации)		
форма обуче	ния очная		
	очная, очно-заочная, заочная		

Рабочая программа практики составлена в соответствии с:

- федеральным государственным образовательным стандартом высшего образования — специалитет по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем», утвержденного приказом Министерства образования и науки Российской Федерации от 26 ноября 2020 г. №1458;
- ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специализация «Управление безопасностью телекоммуникационных систем и сетей», одобренным Ученым советом университета (протокол № 6 «22» февраля 2021г.).

Рабочая программа практики обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специализация «Управление безопасностью телекоммуникационных систем и сетей» на заседании кафедры информационной безопасности «30» августа 2021 г., протокол № 1.

Зав. кафедрой Станы Таныгин М.О.
Разработчик программы к.т.н., доцент (ученая степень и ученое звание, Ф.И.О.)
Директор научной библиотеки Мреме Макаровская В.Г. Рабочая программа практики пересмотрена, обсуждена и рекомендова-
на к реализации в образовательном процессе на основании учебного плана
ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных
систем на основании учебного плана ОПОП ВО 10.05.02 Информационная
безопасность телекоммуникационных систем, специализация «Управление
безопасностью телекоммуникационных систем и сетей», одобренного Уче-
ным советом университета протокол № <u>6 « Д2 »</u>
нии кафедры <u>Иб</u> <u>мотеков в 11 от 30 об 2022</u> .
(наименование кафедры, дата, номер протокола)
Зав. кафедрой
Рабочая программа практики пересмотрена, обсуждена и рекомендова-
на к реализации в образовательном процессе на основании учебного плана
ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных
систем на основании учебного плана ОПОП ВО 10.05.02 Информационная
безопасность телекоммуникационных систем, специализация «Управление
безопасностью телекоммуникационных систем и сетей», одобренного Уче-
ным советом университета протокол № 3 « 27 » _ 02 _ 20 23 г., на заседа-
нии кафельы Mb и политиру он Midous 312 08 2023
(наименование кафедры, дата, номер протокола)
San vadaunoŭ

1 Цель и задачи практики. Указание вида, типа, способа и формы (форм) ее проведения

1.1. Цель практики

Целью производственной преддипломной практики является получение профессиональных умений и опыта профессиональной деятельности в области информационной безопасности в условиях реального производства.

1.2. Задачи практики

- 1. Формирование профессиональных компетенций, установленных ФГОС ВО и закрепленных учебным планом за производственной преддипломной практикой.
- 2. Освоение современных технологий и технических средст, применяемых в области информационной безопасности.
- 3. Совершенствование навыков подготовки, представления и защиты информационных, проектных, аналитических, руководящих и отчетных документов по результатам профессиональной деятельности и практики.
 - 4. Развитие исполнительских и лидерских навыков обучающихся.

1.3 Указание вида, типа, способа и формы (форм) проведения практики

Вид практики – производственная.

Тип практики – преддипломная.

Способ проведения практики – стационарная (в г. Курске) и выездная (за пределами г. Курска).

Практика проводится в профильных организациях, с которыми университетом заключены соответствующие договоры.

Практика проводится в организациях различных отраслей и форм собственности, в органах государственной или муниципальной власти, академических или ведомственных научно-исследовательских организациях, учреждениях системы высшего или дополнительного профессионального образования, деятельность которых связана с вопросами информационной безопасности и соответствует специализации данной образовательной программы: в ФОИВ РФ, ФОИВ субъектов РФ и муниципальных образований, на кафедрах информационной безопасности, обладающих необходимым кадровым и научно-техническим потенциалом, и т.п.

Обучающиеся, совмещающие обучение с трудовой деятельностью, вправе проходить практику по месту трудовой деятельности в случаях, если профессиональная деятельность, осуществляемая ими, соответствует требованиям к содержанию практики, представленному в разделе 4 настоящей программы.

Выбор мест прохождения практики для лиц с ограниченными возможностями здоровья производится с учетом состояния здоровья обучающихся и требований по доступности.

 Φ орма проведения практики — сочетание дискретного проведения практик по видам и по периодам их проведения.

2 Перечень планируемых результатов обучения при прохождении практики, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

Таблица 2 – Результаты обучения по практике

Планируемы	е результаты освоения	Код	Планируемые
	ї профессиональной	и наименование	результаты обучения
	тельной программы	индикатора	по практике,
-	гнции, закрепленные	достижения	соотнесенные с
,	а практикой)	компетенции,	индикаторами
код	наименование	закрепленного	достижения
компетенции	компетенции	за практикой	компетенций
ПК-1	Способен проводить	ПК-1.1	Знать:
	теоретические и	Формулирует тезисы из	основные тенденции в
	экспериментальные	анализируемой научно-	развитии современного
	исследования	технической	информационного
	защищённости	литературы	обществ и проблемы
	телекоммуникационных	1 31	информационной
	систем и сетей		безопасности.
			Уметь:
			использовать
			разнообразные
			источники информации
			для получения новых
			знаний по проблемам
			информационной
			безопасности.
			Владеть:
			Навыками подготовки
			аналитических отчётов
			по актуальным
			проблемам
			информационной
			безопасности.
		ПК-1.2	<i>Знать:</i> принципы
		Разрабатывает	обработки и передачи
		формальные модели	данных в ТКС,
		обработки и передачи	номенклатуру средств
		данных в	обработки данных
		телекоммуникационных	Уметь: на основе
		системах	имеющихся сведений о
		CHCICMAA	имсющился сведении о

7		70	T.
	зультаты освоения	Код	Планируемые
_	офессиональной	и наименование	результаты обучения
-	ьной программы	индикатора	по практике,
, , ,	и, закрепленные	достижения	соотнесенные с
за пра	актикой)	компетенции,	индикаторами
код	наименование	закрепленного	достижения
компетенции	компетенции	за практикой	компетенций
			ТКС формулировать
			абстрактные модели
			циркуляции данных в
			них
			Владеть (или Иметь
			опыт деятельности):
			формализации и
			математической
			интерпретации
			процессов обработки и
			передачи данных в ТКС
		ПК-1.3	Знать:
		Формулирует целевые	основные источники
		критерии для	информации по
		оценивания	профессиональной
		эффективности	тематике.
		исследуемых систем	Уметь:
		песледуемых систем	сопоставлять известные
			методы и средства
			обеспечения
			информационной
			безопасности
			потребностям заказчика
			и условиям конкретного
			объекта.
			Владеть:
			навыками решения
			задач комплексного
			обеспечения
			информационной
			безопасности
			телекоммуникационных
		ПІС 1 Л	систем.
		ПК-1.4	Знать:
		Проводит	Принципы организации
		экспериментальные и	исследований и
		теоретические	процессов
		исследования	телекоммуникационных
		защищённости	систем.
		телекоммуникационных	Уметь:
		систем и сетей	Формулировать задачи,
			планировать и
			проводить исследования
			в сфере
			информационной

Планипуемы	е результаты освоения	Код	Планируемые
	те результиты освоения й профессиональной	и наименование	результаты обучения
	трофессиональной тельной программы	и наименование индикатора	по практике,
_	тельной программы енции, закрепленные	достижения	соотнесенные с
,	а практикой)	компетенции,	индикаторами
код	наименование	закрепленного	достижения
		за практикой	компетенций
компетенции	компетенции	за практикой	безопасности.
			Владеть:
			Навыками
			планирования и проведения
			проведения исследования объектов,
			явлений и процессов
			_
			телекоммуникационных
ПК-6	Caraca	ПК-6.1	систем.
11K-0	Способен управлять		Знать:
	работами по обеспечению	Определяет перечень	Принципы организации
		информации,	телекоммуникационных
	информационной	подлежащей защите	систем и их уязвимости.
	безопасности		Уметь:
			Формулировать
			технические требования
			K
			телекоммуникационным
			системам и мерам по
			предотвращению
			уязвимостей.
			Владеть:
			навыками создания
			моделей угроз и
			моделей
			злоумышленника для
			телекоммуникационных
		HIC CO	систем и устройств.
		ПК-6.2	Знать:
		Определяет требуемый	законы, технологии,
		уровень защищённости	правила, приемы
		информации,	обработки исследования
		циркулирующей в	уровня защищенности
		телекоммуникационной	объектов
		системе	информатизации.
			Уметь:
			подготовить
			развернутый отчет по
			результатам
			обследования объекта.
			Владеть:
			навыками подготовки
			аттестационных
			документов на предмет
			соответствия объекта

		72.	
	е результаты освоения	Код	Планируемые
основной профессиональной		и наименование	результаты обучения
образовательной программы		индикатора	по практике,
(компетенции, закрепленные		достижения	соотнесенные с
	а практикой)	компетенции,	индикаторами
код	наименование	закрепленного	достижения
компетенции	компетенции	за практикой	компетенций
			требованиям по
			информационной
			безопасности.
		THE C 2	2
		ПК-6.3	Знать:
		Определяет меры для	Инструментальные
		защиты в информации в	средства обеспечения
		телекоммуникационных	защиты информации
		системах и сетях	телекоммуникационных
			систем.
			Уметь:
			Осуществлять
			рациональный выбор
			средств обеспечения
			информационной
			безопасности
			телекоммуникационных
			систем.
			Владеть:
			Навыками эксплуатации
			телекоммуникационных
			приборов и средств
			защиты информации.
ПК-7	Способен	ПК-7.1	Знать: структуру и
IIIC /	документально	Разрабатывает	содержание
	обеспечивать процесса	технические задания на	технических заданий на
	защиты информации в	модернизацию систем	проведение работ по
	телекоммуникационных	защиты информации	обеспечению
	системах и сетях	защиты информации	информационной
	системах и сстях		безопасности
			Уметь: формулировать
			задачи и уели
			модернизации системы обеспечения
			информационной безопасности
			Владеть (или Иметь
			опыт деятельности):
			формулирования
			заданий для
			обеспечения
			информационной
			безопасности

Планируемые	е результаты освоения	Код	Планируемые
	профессиональной	и наименование	результаты обучения
	пельной программы	индикатора	по практике,
_	нции, закрепленные	достижения	соотнесенные с
за практикой)		компетенции,	индикаторами
код	наименование	закрепленного	достижения
компетенции	компетенции	за практикой	компетенций
,	,	ПК-7.2	Знать: правила
		Формирует документы	выполнения работ по
		для обоснования	обеспечению
		разработки и	информационной
		модернизации систем	безопасности
		защиты информации	Уметь: документально
		, , ,	описывать
			применяемые для
			обеспечения
			безопасности ТКС
			технологии
			Владеть (или Иметь
			опыт деятельности):
			разработки и
			модернизации систем
			защиты информации
		ПК-7.3	Знать: принципы и
		Разрабатывает модели	структуру моделей
		угроз и модели	угроз и моделей
		нарушителей	нарушителя
			Уметь: соотносить
			уязвимости в
			телекоммуникационных
			системах возможностям
			злоумышленников
			Владеть (или Иметь
			опыт деятельности):
			определения категорий
			злоумышленников
			исходя из
			характеристик
			телекоммуникационных
			систем
		ПК-7.4	<i>Знать:</i> структуру и
		Готовит проекты	состав нормативных
		нормативных и	документов по
		методических	обеспечению
		материалов,	информационной
		регламентирующих	безопасности
		выполнение работ по	Уметь: анализировать
		защите информации	имеющиеся требования
			нормативных
			документов и
			формулировать
			положения по

Планируемы	е результаты освоения	Код	Планируемые
	ї профессиональной	и наименование	результаты обучения
	тельной программы	индикатора	по практике,
*	гнции, закрепленные	достижения	соотнесенные с
,	а практикой)	компетенции,	индикаторами
код	наименование	закрепленного	достижения
компетенции	компетенции	за практикой	компетенций
		1	проведению работ по
			обеспечению
			информационной
			безопасности
			Владеть (или Иметь
			опыт деятельности):
			проведения и
			документального
			обеспечения работ по
			информационной
			безопасности
ПК-8	Способен организовать	ПК-8.1	Знать: порядок
	работы по выполнению	Управляет работой	действий специалистов
	требований защиты	специалистов по	по созданию и
	информации	созданию и	эксплуатации средств
	ограниченного доступа	эксплуатации средств	защиты информации в
	В	защиты информации в	телекоммуникационных
	телекоммуникационных	телекоммуникационных	системах и сетях
	системах и сетях	системах и сетях	Уметь: ставить задачи
			отдельным
			исполнителям при
			создании и
			эксплуатации средств
			защиты информации в
			телекоммуникационных
			системах и сетях
			Владеть (или Иметь
			опыт деятельности):
			созданияю и
			эксплуатации средств
			защиты информации в
			телекоммуникационных
			системах и сетях
		ПК-8.2	Знать: перечень угроз,
		Формирует комплекс	на нейтрализацию
		мер (принципов,	которых направлена та
		правил, процедур,	или иная мера по
		практических приемов,	защите информации
		методов, средств) для	Уметь: объединять
		защиты в	отдельные мероприятия
		телекоммуникационных	по обеспечению
		системах и сетях	информационной
		информации	безопасности в
		ограниченного доступа	логически
		ограни тенного доступа	структурированные
			структурированные

Планипуемые	результаты освоения	Код	Планируемые
	профессиональной	и наименование	результаты обучения
	профессиональной пельной программы	индикатора	по практике,
(компетенции, закрепленные		достижения	соотнесенные с
за практикой)		компетенции,	индикаторами
код	наименование	закрепленного	достижения
компетенции	компетенции	за практикой	компетенций
Компененции	компененции	за практикой	последовательности
			Владеть (или Иметь
			опыт деятельности):
			использования
			отдельных технологий
			обеспечения
			информационной
			безопасности в ТКС
		ПК-8.3	Знать:
		Управляет процессом	административный
		разработки моделей	регламент проведения
		угроз и моделей	работ по обеспечению
		нарушителя	информационной
		безопасности	безопасности
		компьютерных систем	Уметь: принимать
		1	управленческие
			решения при
			проведении работ по
			обеспечению
			информационной
			безопасности
			Владеть (или Иметь
			опыт деятельности):
			разработки моделей
			угроз и моделей
			нарушителя
			безопасности
			компьютерных систем
		ПК-8.4	<i>Знать:</i> основные этапы
		Разрабатывает	жизненного цикла ТКС
		организационно-	и регламентные
		распорядительные	мероприятия на каждом
		документы,	ИЗ НИХ
		регламентирующие	Уметь: выполнять
		порядок эксплуатации	отдельных действий по
		телекоммуникационных	обеспечению
		систем и сетей	информационной
			безопасности
			телекоммуникационных
			систем Владони (или Именя
			Владеть (или Иметь
			опыт деятельности):
			систематизации
			отдельных действий по
			обеспечению

Планируемые результаты освоения основной профессиональной и наименование результаты об образовательной программы (компетенции, закрепленные за практикой) ком наименование компетенции компетенции за практикой за практикой информационной безопасности	учения ке, ые с ми ия
(компетенции, закрепленные за практикой) достижения компетенции, индикатора закрепленного достижени компетенции соотнесенны соотнесенны компетенции, индикатора достижени за практикой компетенции информационной информационном инфо	ые с ми ия
за практикой) компетенции, индикатора код наименование закрепленного достижени компетенции компетенции за практикой компетенци информационной	ми ия
код наименование закрепленного достижени компетенции компетенции за практикой компетенци информационной	ия
код наименование закрепленного достижени компетенции компетенции за практикой компетенци информационной	ия
компетенции компетенции за практикой компетенци информационной	
информационной	ии
телекоммуникац	ионных
систем	
ПК 8.5 Определяет Знать: правовые	е нормы
действия сотрудников действующего	1
при проведении законодательства	a,
мероприятий по регулирующие	
информационной отношения в раз.	пичных
безопасности сферах	
жизнедеятельнос	сти;
Уметь: определя	
направления	
актуализации сис	стемы
защиты информа	ции в
соответствии с	
текущими делові	ыми
потребностями ф	оирмы и
выявленным уро	внем
уязвимости	
защищаемой	
информации;	
Владеть (или Ил	иеть
опыт деятельно	ocmu):
применения	
нормативных пра	авовых
документов в сво	рей
деятельности; -	
навыками работы	ы с
информацией из	
различных источ	ников;
ПК-9 Способен ПК-9.1 Знать: основные	e
эксплуатировать Выявляет сбои и отказы признаки	
телекоммуникационные устройств и программ возникновения с	боев и
системы в защищённом отказов при	
исполнении эксплуатации ТК	
Уметь: в процес	ece
эксплуатации	
фиксировать реж	
работы ТКС, отл	ичные
от штатных	
Владеть (или Ил	
опыт деятельно	-
обнаружения сбо	ев и

Планируемы	е результаты освоения	Код	Планируемые
	профессиональной	и наименование	результаты обучения
образовательной программы		индикатора	по практике,
(компетенции, закрепленные		достижения	соотнесенные с
30	практикой)	компетенции,	индикаторами
код	наименование	закрепленного	достижения
компетенции	компетенции	за практикой	компетенций
,	•	-	отказов реальных ТКС
			1
		ПК-9.2	Знать: знать
		Восстанавливает	номенклатуру
		работоспособность	регламентных работ по
		систем после сбоев и	восстановлению
		отказов устройств и	работоспособности
		программ	устройств и программ
			Уметь: выполнять
			регламентные работы
			по восстановлению
			работоспособности
			устройств и программ
			Владеть (или Иметь
			опыт деятельности):
			эксплуатации
			программного и
			аппартного обеспечения
			ТКС в различных
		HV4.0.0	режимах работы
		ПК-9.3	Знать: назначение и
		Формулирует перечень	классификацию
		действий для	программно-
		восстановления	аппаратных средств ТКС; особенности
		последствий сбоев и	ТКС; особенности функционирования
		отказов	ТКС; классификацию
			программных и
			аппаратных средств
			анализа защищённости
			ТКС, систем
			обнаружения сетевых
			атак, антивирусного
			ПО; технические
			характеристики и
			правила эксплуатации
			средств восстановления
			последствий сбоев и
			отказов.
			Varana
			Уметь: проводить
			мониторинг
			безопасности АС;
			обнаруживать уязвимые
			места в

Планируемые р	езультаты освоения	Код	Планируемые
основной профессиональной образовательной программы		и наименование	результаты обучения
		индикатора	по практике,
(компетенции, закрепленные		достижения	соотнесенные с
за пр	рактикой)	компетенции,	индикаторами
код	наименование	закрепленного	достижения
компетенции	компетенции	за практикой	компетенций
	·		функционировании ПО
			и оборудования ТКС;
			провести настройку ПО
			и оборудования ТКС.
			Владеть: навыками
			настройки
			программных и
			аппаратных средств
			анализа защищённости
			ТКС, систем
			обнаружения сетевых
			атак, антивирусного
			ПО.
		ПК-9.4	<i>Знать:</i> основные
		Регистрирует	признаки
		сообщения об ошибках	возникновения ошибок
		в сетевых устройствах и	в сетевых устройствах и
		операционных системах	операционных системах
			Уметь: в процессе
			эксплуатации
			фиксировать режимы
			работы сетевых
			устройств и
			операционных систем,
			отличные от штатных
			Владеть (или Иметь
			опыт деятельности): навыками обнаружения
			сбоев и отказов
			реальных сетевых
			устройств и
			операционных систем
		ПК-9.5	Знать: структуру и
		Формирует отчёты по	содержание журналов
		результатам работ	аудита
		системы мониторинга	информационной
		1	безопасности
			Уметь: использовать
			технические средства
			ведения журналов
			аудита
			информационной
			безопасности
			Владеть (или Иметь

Планируемые результать освоения основной профессиональной и и наименование индикатора достижения компетенции закрепленые за практикой) код наименование компетенции компетенции закрепленного за практикой достижения компетенции оплатик обезопасности для реализации политик безопасности и программных компонент телекоммуникационной системы уметь: в программных компонентах телекоммуникационной системы уметь: в программных компонентах телекоммуникационной системы. Уметь: в программных компонентах телекоммуникационной системы уметь: в программных компонентах телекоммуникационной системы. Владеть (сили иметь в программных компонентах телекоммуникационной системы. Владеть (сили иметь в программных компонентах телекоммуникационной системы. Владеть (сили иметь в программных компонентах телекоммуникационной системы. Владеть (си			T :	
образовательной программы (компетенции, закрепленные за практикой) код наименование компетенции компетенции закрепленного за практикой информационной безопасности для реализации политик безопасности для реализации для дработы программных компонент телекоммуникационной системы уметь: в процессе эксплуатации фиксировать режимы работы программных компонента телекоммуникационной системы Влафеть (пли Иметь опыт деятьности): навыками обцаружения сбоев и отказов в программных компонентах телекоммуникационной системы Влафоть (пли Иметь опыт деятьности): навыками обцаружения сбоев и отказов в программных компонентах телекоммуникационной системы Влафоть (пли Иметь опыт деятьности): навыками обцаружения сбоев и отказов в программных компонентах телекоммуникационной системы Влафоть (пли Иметь опыт деятьных Влафоть (пли Иметь опыт деятьных Влафоть) для дработы профрамции телекоммуникационных систем. IIK-10.2		- •	Код	Планируемые
Способен	= =			1 2
код код наименование компетенции закрепленного уза практикой наименование компетенции закрепленного уза практикой компетенций динформационной безопасности для реализации политик безопасности для деятельности для реализации политик безопасности для деятельности дл			1	-
ком компетенции за практикой достижения компетенций достижения дости	(компетенции, закрепленные		достижения	
жомпетенции компетенции за практикой компетенций опыт деятельностии; павыками апализа журналов аудита информационной безопасности для реализации политик безопасности и телекоммуникационной системы уметь: в процессе эксплуатации фиксировать режимы работы программных компонент телекоммуникационной системы уметь: в процессе эксплуатации фиксировать режимы работы программных компонентах телекоммуникационной системы, отличные от штатных Владеть (или Иметь опыт деятельности); навыками объявления опиток компонентах телекоммуникационной системы, отличные от штатных Владеть (или Иметь опыт деятельности); навыками объявления опиток компонентах телекоммуникационной системы. Владеть (или Иметь опыт деятельности); навыками объявная об		а практикой)	1	-
ПК-10 Способен эксплуатировать средства обеспечения информационной безопасности Проверяет корректность работы программных компонент телекоммуникационной системы НК-10.1 Проверяет корректность работы программных компонент телекоммуникационной системы НК-10.2 ПК-10.2 Определяет соответствие текущего функционала системы Требованиям профилей защиты ПК-10.2 ПК-10.2 ПК-10.2 Профили защиты информации телекоммуникационной системы уметь: в процессе эксплуатации фиксировать режимы работы программных компонент телекоммуникационной системы, отличные от штатных Влафеты (или Иметь опыть деятельностии): павыками обпаружения сбоев и отказов в программных компонентах телекоммуникационной системы. Профили защиты инструментальные средства обеспечения защиты инструментальные осредства обеспечения защиты информации телекоммуникационных системь. Уметь: Осуществлять рациональный выбор средств реализации профилей защиты. Влафеты: Навыками работы с	код	наименование	закрепленного	достижения
ПК-10 Способен эксплуатировать средства обеспечения информационной безопасности программных компонент треализации политик безопасности телекомуникационной системы информационной системы уметь: в процессе эксплуатации фиксировать режимы работы программных компонент телекомуникационной системы, отличные от штатных вамоеть (или Иметь опыт деятельности): навыками обнаружения сбоев и отказов в программных компонентах телекомуникационной системы, отличные от штатных вамоеть (или Иметь опыт деятельности): навыками обнаружения сбоев и отказов в программных компонентах телекомуникационной системы. ПК-10.2 Определяет соответствие текущего функционала системы требованиям профилей защиты инструментальные средства обеспечения защиты информации телекомуникационных систем. Уметь: Осуществлять рациональный выбор средств реализации профилей защиты. Валоеть: Навыками работы с	компетенции	компетенции	за практикой	компетенций
ПК-10 Способен эксплуатировать средства обеспечения информационной безопасности для реализации политик безопасности ПК-10 ПК-10.1 Проверяет корректность работы программных компонент телекоммуникационной системы потраммных компонент телекоммуникационной системы ПК-10.2 ПК-10.2 Определяет соответствие текущего функционала системы требованиям профилей защиты ПК-10.2 Определяет соответствие текущего функционала системы телекоммуникационной системы. Профили защиты пребованиям профилей защиты ПК-10.2 Определяет соответствие текущего функционала системы требованиям профилей защиты профилей защиты. Владеты: ПК-10.2 Определяет соответствие текущего функционала системы телекоммуникационных системы. Профили защиты профили защиты профилей защиты. Владеты: Осуществлять рапиональный выбор средств реализации профилей защиты. Владеты: Навыками работы с				опыт деятельности):
ПК-10 Способен эксплуатировать средства обеспечения информационной безопасности программных компонент телекоммуникационной системы компонент телекоммуникационной системы уметь: в процессе эксплуатации фиксировать режимы работы программных компонент телекоммуникационной системы уметь: в процессе эксплуатации фиксировать режимы работы программных компонент телекоммуникационной системы, отличные от питатных владеть (или Иметь опыт делеками обнаружения сбоев и отказов в программных компонент телекоммуникационной системы, отличные от питатных владеть (или Иметь опыт делекаму обнаружения сбоев и отказов в программных компонент телекоммуникационной системы опыт делекаму обнаружения сбоев и отказов в программных компонент телекомуникационной системы образованиям профилей защиты инструментальные средства обеспечения защиты инструментальные средства обеспечения защиты информации телекомуникационных систем. Уметь: Осуществлять рациональный выбор средств реализации профилей защиты. Владеть: Осуществлять рациональный выбор средств реализации профилей защиты. Владеть: Навыками работы с				навыками анализа
ПК-10 Способен эксплуатировать средства обеспечения информационной безопасности для реализации политик безопасности Телекоммуникационной системы Телекоммуникационной системы, отличные от штатных Владеть (или Иметь опыт деямения соответствие текущего функционала системы требованиям профилей защиты ПК-10.2 Определяет соответствие текущего функционала системы требованиям профилей защиты ПК-10.2 Определяет соответствие текущего функционала системы требованиям профилей защиты инструментальные средства обеспечения защиты телекоммуникационных смигонент инструментальные средства обеспечения защиты инструментальные средства обеспечения защиты телекоммуникационных системы. Уметь: Осуществлять рациональный выбор средств реализации профилей защиты. Владеть: Навыками работы с				1
ПК-10 Способен эксплуатировать средства обеспечения информационной безопасности для реализации политик безопасности ПК-10.1 Проверяет корректность работы программных компонент телекоммуникационной системы компонент телекоммуникационной системы компонент телекоммуникационной системы компонент телекоммуникационной системы компонентах телекоммуникационной системы, уметь: в программных компонент телекоммуникационной системы, отличные от штатных владеть (или Иметь опыт деятельности): павыками обпаружения сбоев и отказов в программных компонентах телекоммуникационной системы ПК-10.2 Определяет соответствие текущего функционала системы требованиям профилей защиты защиты ПК-10.2 Определяет соответствие текущего функционала системы требованиям профилей защиты инструментальные средства обеспечения защиты инструментальные обеспечения защиты инструментальные обеспечения защиты инструментальные обеспечения защи				
Проверяет корректность работы программных компонент телекоммуникационной системы Программных компонент телекоммуникационной системы Телекоммуникационной системы, отличные от штатных Владеть (или Иметь опыт деятельности): павыками обпаружения сбоев и отказов в программных компонентах телекоммуникационной системы. ТК-10.2 Определяет соответствие текущего функционала системы Требованиям профилей защиты Телекоммуникационной системы знагиты инструментальные средства обеспечения защиты инструментальные средства обеспечения защиты информации телекоммуникационных систем. Тистемы Тистемомуникационной системы Тистемы Тистемомуникационной Системы Тистемы Тистемомуникационной Системы Тистемы Тистемы				безопасности
редства обеспечения информационной безопасности для реализации политик безопасности везопасности компонент телекоммуникационной системы телекоммуникационной системы телекоммуникационной системы уметь: в программных компонент телекоммуникационной системы уметь: в пропредеминых компонент телекоммуникационной системы, отличные от штатных владеть (или Иметь опыт деятельности): навыками обнаружения сбоев и отказов в программных компонентах телекоммуникационной системы ПК-10.2 Определяет соответствие текущего функционала системы требованиям профилей защиты инструментальные средства обеспечения защиты информации телекоммуникационных систем. уметь: Осуществлять рациональный выбор средств реализации профилей защиты. Владеть: Навыками работы с	ПК-10	Способен	ПК-10.1	<i>Знать:</i> основные
программных компонент телекоммуникационной системы в программных компонентах телекоммуникационной системы уметь: в процессе эксплуатации фиксировать режимы работы программных компонент телекоммуникационной системы, отличные от штатных Владеть (или Иметь опыт деятельности): навыками обнаружения сбоев и отказов в программных компонентах телекоммуникационной системы. ПК-10.2 Определяет соответствие текущего функционала системы требованиям профилей защиты информации телекоммуникационных систем. Уметь: Осуществлять рациональный выбор средств реализации профилей защиты. Владеть: Навыками работы с		1		признаки
безопасности для реализации политик безопасности компонент телекоммуникационной системы компонентах телекоммуникационной системы, отличные от штатных компонентах компонентах телекоммуникационной системы опыт деятельности работы программных компонентах компонентах телекоммуникационной системы опыт деятельности работы программных компонент телекоммуникационной системы ПК-10.2 Определяет соответствие текущего функционала системы телекоммуникационной системы защиты информации телекоммуникационных системь. уметь: Осуществлять рациональный выбор средств реализации профилей защиты. Владеть: Навыками работы с		средства обеспечения	корректность работы	возникновения ошибок
реализации политик безопасности телекоммуникационной системы телекоммуникационной системы уметь: в процессе эксплуатации фиксировать режимы работы программных компонент телекоммуникационной системы, отличные от штатных Владеть (или Иметь опыт деятельностии): навыками обнаружения сбоев и отказов в программных компонентах телекоммуникационной системы ПК-10.2 Определяет соответствие текущего функционала системы требованиям профилей защиты информации телекоммуникационных систем. Уметь: Осуществлять рациональный выбор средств реализации профилей защиты. Владеть: Навыками работы с		информационной	программных	в программных
системы системы системы уметь: в процессе эксплуатации фиксировать режимы работы программных компонент телекоммуникационной системы, отличные от штатных Владеть (или Иметь опыт деятельности): навыками обнаружения сбоев и отказов в программных компонентах телекоммуникационной системы ПК-10.2 Определяет соответствие текущего функционала системы требованиям профилей защиты профилей защиты информации телекоммуникационных систем. уметь: Осуществлять рациональный выбор средств реализации профилей защиты. Владеть: Навыками работы с		безопасности для	компонент	компонентах
уметь: в процессе эксплуатации фиксировать режимы работы программных компонент телекоммуникационной системы, отличные от штатных Владеть (или Иметь опыт деятельностии): навыками обнаружения сбоев и отказов в программных компонентах телекоммуникационной системы Знать: ПК-10.2 Определяет соответствие текущего функционала системы требованиям профилей защиты инструментальные средства обеспечения защиты информации телекоммуникационных систем. Уметь: Осуществлять рациональный выбор средств реализации профилей защиты. Владеть: Навыками работы с		=	телекоммуникационной	телекоммуникационной
эксплуатации фиксировать режимы работы программных компонент телекоммуникационной системы, отличные от штатных Владеты (или Иметь опыт деятельности): навыками обнаружения сбоев и отказов в программных компонентах телекоммуникационной системы ПК-10.2 Определяет соответствие текущего функционала системы требованиям профилей защиты инструментальные средства обеспечения защиты информации телекоммуникационных систем. Уметь: Осуществлять рациональный выбор средств реализации профилей защиты. Владеть: Навыками работы с		безопасности	системы	системы
фиксировать режимы работы программных компонент телекоммуникационной системы, отличные от штатных Владеть (или Иметь опыт деятельности): навыками обнаружения сбоев и отказов в программных компонентах телекоммуникационной системы ПК-10.2 Определяет соответствие текущего функционала системы требованиям профилей защиты инструментальные средства обеспечения защиты информации телекоммуникационных систем. Уметь: Осуществлять рациональный выбор средств реализации профилей защиты. Владеть: Навыками работы с				<i>Уметь:</i> в процессе
работы программных компонент телекоммуникационной системы, отличные от штатных Владеты (или Иметь опыт деятельности): навыками обнаружения сбоев и отказов в программных компонентах телекоммуникационной системы ПК-10.2 Определяет соответствие текущего функционала системы требованиям профилей защиты информации телекоммуникационных систем. Уметь: Осуществлять рациональный выбор средств реализации профилей защиты. Владеть: Навыками работы с				_
компонент телекоммуникационной системы, отличные от штатных Владеть (или Иметь опыт деятельности): навыками обнаружения сбоев и отказов в программных компонентах телекоммуникационной системы ПК-10.2 Определяет соответствие текущего функционала системы требованиям профилей защиты Телекоммуникационной системы Профили защиты инструментальные средства обеспечения защиты информации телекоммуникационных систем. Уметь: Осуществлять рациональный выбор средств реализации профилей защиты. Владеть: Навыками работы с				
телекоммуникационной системы, отличные от штатных Владеть (или Иметь опыт деятельности): навыками обнаружения сбоев и отказов в программных компонентах телекоммуникационной системы ПК-10.2 Определяет соответствие текущего функционала системы требованиям профилей защиты инструментальные средства обеспечения защиты информации телекоммуникационных систем. Уметь: Осуществлять рациональный выбор средств реализации профилей защиты. Владеть: Навыками работы с				работы программных
системы, отличные от штатных Владеть (или Иметь опыт деятельностии): навыками обнаружения сбоев и отказов в программных компонентах телекоммуникационной системы ПК-10.2 Определяет соответствие текущего функционала системы требованиям профилей защиты инструментальные средства обеспечения защиты информации телекоммуникационных систем. Уметь: Осуществлять рациональный выбор средств реализации профилей защиты. Владеть: Навыками работы с				компонент
ПК-10.2 Определяет соответствие текущего функционала системы требованиям профилей защиты защиты телекоммуникационных системы требованиям профилей защиты информации телекоммуникационных систем. уметь: Осуществлять рациональный выбор средств реализации профилей защиты. Владеть: Навыками работы с				телекоммуникационной
Владеть (или Иметь опыт деятельности): навыками обнаружения сбоев и отказов в программных компонентах телекоммуникационной системы ПК-10.2 Определяет соответствие текущего функционала системы требованиям профилей защиты инструментальные средства обеспечения защиты информации телекоммуникационных систем. Уметь: Осуществлять рациональный выбор средств реализации профилей защиты. Владеть: Навыками работы с				системы, отличные от
опыт деятельности): навыками обнаружения сбоев и отказов в программных компонентах телекоммуникационной системы ПК-10.2 Определяет соответствие текущего функционала системы требованиям профилей защиты телекоммуникационных средства обеспечения защиты информации телекоммуникационных систем. Уметь: Осуществлять рациональный выбор средств реализации профилей защиты. Владеть: Навыками работы с				штатных
навыками обнаружения сбоев и отказов в программных компонентах телекоммуникационной системы ПК-10.2 Определяет соответствие текущего функционала системы требованиям профилей защиты информации телекоммуникационных систем. Уметь: Осуществлять рациональный выбор средств реализации профилей защиты. Владеть: Навыками работы с				
сбоев и отказов в программных компонентах телекоммуникационной системы ПК-10.2 Определяет соответствие текущего функционала системы требованиям профилей защиты информации телекоммуникационных систем. Уметь: Осуществлять рациональный выбор средств реализации профилей защиты. Владеть: Навыками работы с				опыт деятельности):
ПК-10.2 Определяет соответствие текущего функционала системы требованиям профилей защиты телекоммуникационной системы Профили защиты инструментальные средства обеспечения защиты информации телекоммуникационных систем. Уметь: Осуществлять рациональный выбор средств реализации профилей защиты. Владеть: Навыками работы с				навыками обнаружения
ТК-10.2 Знать: Определяет соответствие текущего функционала системы требованиям профилей защиты информации телекоммуникационных систем. Уметь: Осуществлять рациональный выбор средств реализации профилей защиты. Владеть: Навыками работы с				сбоев и отказов в
ТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМЫ ПК-10.2 Определяет соответствие текущего функционала системы требованиям профилей защиты информации телекоммуникационных систем. Уметь: Осуществлять рациональный выбор средств реализации профилей защиты. Владеть: Навыками работы с				программных
ПК-10.2 Определяет соответствие текущего функционала системы требованиям профилей защиты защиты телекоммуникационных систем. уметь: Осуществлять рациональный выбор средств реализации профилей защиты. Владеть: Навыками работы с				компонентах
ПК-10.2 Определяет соответствие текущего функционала системы требованиям профилей защиты телекоммуникационных систем. Уметь: Осуществлять рациональный выбор средств реализации профилей защиты. Владеть: Навыками работы с				телекоммуникационной
Определяет соответствие текущего функционала системы требованиям профилей защиты информации телекоммуникационных систем. Уметь: Осуществлять рациональный выбор средств реализации профилей защиты. Владеть: Навыками работы с				системы
соответствие текущего функционала системы требованиям профилей защиты информации телекоммуникационных систем. Уметь: Осуществлять рациональный выбор средств реализации профилей защиты. Владеть: Навыками работы с			ПК-10.2	Знать:
функционала системы требованиям профилей защиты информации телекоммуникационных систем. Уметь: Осуществлять рациональный выбор средств реализации профилей защиты. Владеть: Навыками работы с			Определяет	
требованиям профилей защиты информации телекоммуникационных систем. Уметь: Осуществлять рациональный выбор средств реализации профилей защиты. Владеть: Навыками работы с				1 0
защиты телекоммуникационных систем. Уметь: Осуществлять рациональный выбор средств реализации профилей защиты. Владеть: Навыками работы с				
систем. Уметь: Осуществлять рациональный выбор средств реализации профилей защиты. Владеть: Навыками работы с			требованиям профилей	защиты информации
Уметь: Осуществлять рациональный выбор средств реализации профилей защиты. Владеть: Навыками работы с			защиты	телекоммуникационных
Осуществлять рациональный выбор средств реализации профилей защиты. Владеть: Навыками работы с				систем.
рациональный выбор средств реализации профилей защиты. Владеть: Навыками работы с				
средств реализации профилей защиты. <i>Владеть:</i> Навыками работы с				_
профилей защиты. Владеть: Навыками работы с				_
Владеть: Навыками работы с				
Навыками работы с				
профилями защиты.				Навыками работы с
				профилями защиты.

Планируемые результаты освоения		Код	Планируемые
основной профессиональной		и наименование	результаты обучения
образовательной программы		индикатора	по практике,
(компетенции, закрепленные		достижения	соотнесенные с
за практикой)		компетенции,	индикаторами
код	наименование	закрепленного	достижения
компетенции	компетенции	за практикой	компетенций
		ПК-10.3	Знать: основные этапы
		Формирует	жизненного цикла ТКС
		систематизированные	и регламентные
		политики	мероприятия на каждом
		информационной	из них
		безопасности	Уметь:
			Владеть (или Иметь
			опыт деятельности):
			систематизации
			отдельных действие по
			обеспечению
			информационной
			безопасности
			телекоммуникационных
			систем
		ПК-10.4	Знать: Структуру и
		Разрабатывает профили	содержание профилей
		заданий по	заданий по
		безопасности для	безопасности для
		оборудования	оборудования
		телекоммуникационных	телекоммуникационных
		систем в защищённом	систем в защищённом
		исполнении	исполнении
			Уметь:
			структурировать
			отдельные процедуры и
			регламентные работы в
			единые
			систематические
			профили безопасности
			Владеть (или Иметь
			опыт деятельности):
			навыками эксплуатации
			оборудования
			телекоммуникационных
			систем в защищённом
ПК-11	Способы удрогият	ПК-11.1	исполнении Знать: особенности
1118-11	Способен управлять		
	жизненным циклом подсистем обеспечения	Определяет действия по обеспечению	различных этапов
			жизненного цикла ТКС
	информационной безопасности	информационной безопасности на	Уметь: исходя их
	осзопасности		имеющегося перечня
		различных этапах	угроз реализовывать
		жизненного цикла	технологии обеспечения
		телекоммуникационной	информационной

Планируот	a nanna mama aaaaana	Код	Планируелиле
	е результаты освоения		Планируемые
основной профессиональной		и наименование	результаты обучения
образовательной программы		индикатора	по практике,
(компетенции, закрепленные		достижения	соотнесенные с
	практикой)	компетенции,	индикаторами
код	наименование	закрепленного	достижения
компетенции	компетенции	за практикой	компетенций
		системы	безопасности
			Владеть (или Иметь
			опыт деятельности):
			эксплуатации ТКС на
			различных этапах
		HIC 11.0	жизненного цикла
		ПК-11.2	<i>Знать:</i> перечень
		Выбирает перечень	реализуемых
		реализуемых	телекоммуникационной
		телекоммуникационной	системой технологий
		системой технологий	для удовлетворения
		для удовлетворения	требований по
		требований по	информационной безопасности
		информационной безопасности	
		оезопасности	Уметь: соотносить
			технологии
			информационной
			безопасности
			существующим в ТКС
			уязвимостям
			Владеть (или Иметь
			опыт деятельности):
			реализации технологий
			информационной
		ПК 11.2	безопасности
		ПК-11.3	Знать: критерии
		Оценивает результат	результативности
		применения штатных	применения штатных
		средств обеспечения	средств обеспечения
		информационной безопасности	информационной безопасности
		ОСЗОПАСНОСТИ	Уметь: формулировать
			количественные
			критерии
			результативности применения штатных
			средств обеспечения
			информационной
			безопасности
			Владеть (или Иметь
			опыт деятельности):
			навыками оценки
			результативности
			применения штатных
			средств обеспечения

Планируемые результаты освоения		Код	Планируемые
основной профессиональной		и наименование	результаты обучения
образовап	пельной программы	индикатора	по практике,
(компете	нции, закрепленные	достижения	соотнесенные с
3 <i>a</i>	практикой)	компетенции,	индикаторами
код	наименование	закрепленного	достижения
компетенции	компетенции	за практикой	компетенций
			информационной
			безопасности
		ПК-11.4	<i>Знать:</i> меры и
		Формулирует	технологии,
		предложения по	направленные на
		совершенствованию	повышение
		подсистем обеспечения	защищённости
		информационной	процессов обработки
		безопасности	информации в ТКС
			<i>Уметь:</i> определять
			меры и технологии,
			направленные на
			повышение
			защищённости
			процессов обработки
			информации в
			конкретной ТКС
			Владеть (или Иметь
			опыт деятельности):
			обеспечения процесса
			защиты информации в
			TKC

3 Указание места практики в структуре основной профессиональной образовательной программы. Указание объема практики в зачетных единицах и ее продолжительности в неделях либо в академических или астрономических часах

Производственная технологическая практика входит часть, образовательных формируемую участниками отношений блока «Практика» основной профессиональной образовательной программы – 10.05.02 Информационная программы специалитета безопасность телекоммуникационных систем, специализация «Управление безопасностью телекоммуникационных систем и сетей». Практика проходит на 6 курсе в 11 семестре.

Объем производственной преддипломной практики, установленный учебным планом, – 9 зачетных единиц, продолжительность – 6 недель (324 часа).

4 Содержание практики

Практика проводится в форме контактной работы и в иных формах, установленных университетом (работа обучающегося на рабочем месте в профильной организации; ведение обучающимся дневника практики; составление обучающимся отчета о практике; подготовка обучающимся презентации; подготовка обучающегося к защите отчета о практике и ответу на вопросы комиссии на промежуточной аттестации по практике).

Контактная работа по практике (включая контактную работу по промежуточной аттестации по практике) составляет 6 часов, работа обучающегося в иных формах — 318 часов.

Содержание практики уточняется для каждого обучающегося в зависимости от специфики конкретной профильной организации, являющейся местом ее проведения, и выдается в форме задания на практику.

Таблица 4 – Этапы и содержание практики

No	Этапы практики	Содержание практики	Трудоемкость
Π/Π	_		(час)
1	Подготовительный	Решение организационных	2
	этап	вопросов:	
		1) распределение обучающихся по	
		местам практики;	
		2) знакомство с целью, задачами,	
		программой, порядком	
		прохождения практики;	
		3) получение заданий от	
		руководителя практики от	
		университета;	
		4) информация о требованиях к	
		отчетным документам по	
		практике;	
		5) первичный инструктаж по	
		технике безопасности.	
2	Основной этап	Работа обучающихся в	186
		профильной организации	
2.1	Знакомство с	Знакомство с профильной	2
	профильной	организацией, руководителем	
	организацией	практики от организации,	
		рабочим местом и должностной	
		инструкцией.	5
		Инструктаж по технике	
		безопасности на рабочем месте.	

		Знакомство с содержанием	
		деятельности профильной	
		организации по обеспечению	
		информационной безопасности и	
		проводимыми в нем	3
		мероприятиями.	3
		Изучение нормативных правовых	
		актов профильной организации по	
		обеспечению информационной	
		безопасности (политика	
		безопасности профильной	
		организации, положения,	
		приказы, инструкции,	
		должностные обязанности,	
		памятки и др.).	
2.2	Практическая	Самостоятельное проведение	90.
	подготовка	мониторинга и (или)	
	обучающихся	производственного контроля	
	(непосредственное	эффективности применения	
	выполнение	средств защиты информации в	
	обучающимися	TKC.	
	видов работ,	Организация работы 2-3 человек и	
	связанных с	руководство их работой в	
	будущей	процессе проведения мониторинга	
	профессиональной	безопасности ТКС.	
	деятельностью)	Создание плана работы	
		коллектива из $3-4$ человек,	
		реализующего политику	
		безопасности в ТКС	
		Самостоятельная обработка и	
		систематизация полученных	
		данных с помощью	
		профессиональных программных	
		комплексов и информационных	
		технологий.	
		Организация работы 2-3 человек	
		и руководство их работой в	
		процессе обработки и	
		систематизации полученных	
		данных.	
		Представление результатов	
		мониторинга руководителю	
		практики от организации	
		Самостоятельное проведение	
	l	1	

		анализа результатов проведенного	
		мониторинга информационной	
		безопасности.	
		Организация работы 2-3 человек и	
		руководство их работой в	
		процессе работ по обеспечению	
		информационной безопасности.	
		Оценка рисков информационной	
		безопасности.	
		Представление результатов	
		анализа и обоснование оценки	
		руководителю практики от	
		организации.	
		Самостоятельная подготовка	
		рекомендаций по повышению	
		уровня информационной	
		безопасности предприятия.	
		Организация работы 2-3 человек	
		и руководство их работой в	
		процессе подготовки	
		рекомендаций по повышению	
		уровня информационной	
		безопасности предприятия.	
		Представление своих	
		рекомендаций руководителю	
		практики от организации.	
		Самостоятельное составление	
		краткосрочного плана раболт по	
		обеспечению безопасности	
		организации, эксплуатирующей ТКС.	
		Организация работы 2-3 человек	
		и руководство их работой в	
		процессе составления	
		краткосрочного и долгосрочного	
		прогнозов.	
		Представление своего прогноза с	
		обоснованием руководителю	
		практики от организации.	
3	Заключительный	Оформление дневника практики.	36
	этап	Составление отчета о практике.	
		Подготовка графических	
		материалов для отчета.	
		Представление дневника практики	

и защита отчета о практике на	
промежуточной аттестации.	

5 Указание форм отчетности по практике

Формы отчетности студентов о прохождении производственной производственной практики:

- дневник практики (форма дневника практики приведена на сайте университета https://www.swsu.ru/structura/umu/training_division/blanks.php),
 - отчет о практике.

Структура отчета о производственной преддипломной практике:

- 1) Титульный лист.
- 2) Содержание.
- 3) Введение. Цель и задачи практики. Общие сведения о предприятии, на котором проходила практика.
 - 4) Основная часть отчета.
- Характеристика деятельности предприятия по обеспечению информационной безопасности и проводимых в нем мероприятий.
- Основные нормативные правовые акты предприятия по обеспечению информационной безопасности.
 - Анализ результатов мониторинга.
 - Оценка рисков информационной безопасности ТКС.
- Рекомендации по повышению уровня информационной безопасности предприятия.
 - Краткосрочный и долгосрочный прогноз развития ситуации.
- 5) Заключение. Выводы о достижении цели и выполнении задач практики.
 - 6) Список использованной литературы и источников.
 - 7) Приложения (иллюстрации, таблицы, карты и т.п.).

Отчет должен быть оформлен в соответствии с:

- ГОСТ Р 7.0.12-2011 Библиографическая запись. Сокращение слов и словосочетаний на русском языке. Общие требования и правила.
- ГОСТ 2.316-2008 Единая система конструкторской документации. Правила нанесения надписей, технических требований и таблиц на графических документах. Общие положения;
- ГОСТ 7.32-2001 Отчет о научно-исследовательской работе.
 Структура и правила оформления;
 - ГОСТ 2.105-95 ЕСКД. Общие требования к текстовым документам;
- ГОСТ 7.1-2003 Система стандартов по информации, библиотечному и издательскому делу. Общие требования и правила составления;

- ГОСТ 2.301-68 Единая система конструкторской документации.
 Форматы;
- ГОСТ 7.82-2001 Библиографическая запись. Библиографическое описание электронных ресурсов. Общие требования и правила составления;
- ГОСТ 7.9-95 (ИСО 214-76). Система стандартов по информации, библиотечному и издательскому делу. Реферат и аннотация. Общие требования.
- СТУ 04.02.030-2015 «Курсовые работы (проекты). Выпускные квалификационные работы. Общие требования к структуре и оформлению».

6 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по практике

6.1 Перечень компетенций с указанием этапов их формирования в процессе освоения основной профессиональной образовательной программы

Таблица 6.1 – Этапы формирования компетенций

Код и	Этапы* формирования компетенций и дисциплины (модули), практики,			
наименование	НИР, при изучении которых формируется данная компетенция			
компетенции	начальный	основной	завершающий	
1	2	3	4	
ПК-1	Квантовая и оптическая	Производственная предди	пломная практика	
	электроника			
	Физические основы			
	оптических систем			
	СВЯЗИ			
ПК-6	Комплексная защита	Производственная преддин	пломная практика	
	объектов			
	информатизации			
ПК-7	Порядок проведения	Производственная преддин	пломная практика	
	аттестации объектов			
	информатизации			
ПК-8	Организация и	Порядок проведения	Производственная	
	управление службой	аттестации объектов	преддипломная	
	защиты информации	информатизации	практика	
	Система сертификации			
	и лицензирования			
	деятельности по защите			
	информации			
ПК-9	Комплексная защита	Производственная преддин	пломная практика	
	объектов			
	информатизации			
ПК-10	Информационная	Инфокоммуникационные	Производственная	
	безопасность	системы навигации и	преддипломная	
	телекоммуникационных	диспетчеризации и их	практика	

	систем	защита Безопасность средств мониторинга территорий и объектов	
ПК-11	Комплексная защита объектов информатизации	Производственная предди	пломная практика

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

Таблица 6.2 – Показатели и критерии оценивания компетенций, шкала оценивания

компетенц ии/ этап (указывает ся название этапа из п. 6.1) Пороговый уровень (сорошо») Пороговый уровень (сорошо») Пороговый уровень (сорошо») Поровень (сорошо») Порошо нетененция в развити современного обществ и проблемы информационной безопасности. Поровень (сорошо») Порошо нетененция варити поровень (сорошо») Поровень (сорошо нетененция варити поровень (сорошо») Порошо нетененция варити поровень (сорошо») Порошо нетененция варити поровемного обществ и проблемы информационной безопасности. Поровень (странация на сененция варити поровемного обществ и проблемы информационной безопасности. Поровень (странация на сененция варити поровемного обществ и проблемы информационной безопасности. Поровень (странация на сененция варити поровемного обществ и проблемы информационной безоп	Код	Показатели	Критерии и шкала оцег	нивания компетенций	
ПК-1/ завершаю щий ПК-1.1 формулиру ет тезисы из анализируе мой научно- техническо й литературы Птературы Потубокие знания о Тенденциях в Потувании Современного Проблемы Проблемы Предатура Птературы Птература Птература Птературы Птературы Птературы Птература Птературы Птературы	ии/ этап (указывает ся название этапа из	компетенций (индикаторы достижения компетенций , закрепленные за	уровень	уровень	
завершаю щий Формулиру ет тезисы из анализируе мой научнотехническо й литературы Пуметь: Сформированное умение использовать разнообразные источники информации для проблемам информационной безопасности. Владеть (или владеть (или проблемам информационной безопасности. Умеренно владеет	1		3	4	5
деятельности): Владеть (или подготовки	завершаю	Формулиру ет тезисы из анализируе мой научнотехническо й	Фрагментарные знания о тенденциях в развитии современного информационного обществ и проблемы информационной безопасности. Уметь: Сформированное умение использовать разнообразные источники информации для получения новых знаний по проблемам информационной безопасности. Владеть (или Иметь опыт	Сформированные, но содержащие отдельные пробелы знания о тенденциях в развитии современного информационного обществ и проблемы информационной безопасности. Уметь: Сформированное умение использовать разнообразные источники информации для получения новых знаний по проблемам информационной безопасности.	Глубокие знания о тенденциях в развитии современного информационного обществ и проблемы информационной безопасности. Уметь: Уверенно и на высоком уровне использовать разнообразные источники информации для получения новых знаний по проблемам информационной безопасности. Владеть: Уверенно владеет навыками

1	2	3	4	5
		Владеет базовыми	Иметь опыт	аналитических
		навыками	деятельности):	отчётов по
		подготовки	Владеет основными	актуальным
		аналитических	навыками	проблемам
		отчётов по	подготовки	информационной
		актуальным	аналитических	безопасности.
		проблемам	отчётов по	
		информационной	актуальным	
		безопасности.	проблемам	
			информационной	
		_	безопасности.	
	ПК-1.2	Знать:	Знать:	<i>Знать:</i> Глубокие
	Разрабатыва	Фрагментарные	Сформированные,	знания о
	ет	знания о	но содержащие	принципах
	формальные	принципах	отдельные пробелы	обработки и
	модели	обработки и	знания о	передачи данных в
	обработки и	передачи данных в	принципах	ТКС, номенклатуру
	-	ТКС, номенклатуру	обработки и	средств обработки
	передачи	средств обработки	передачи данных в	данных Уматы Урараную
	данных в	данных	ТКС, номенклатуру	Уметь: Уверенно
	телекоммун	Уметь:	средств обработки	и на высоком
	икационных	Сформированное	данных	уровне на основе
	системах	умение на основе имеющихся	Уметь: Сформированное	имеющихся сведений о ТКС
		сведений о ТКС	умение на основе	формулировать
		формулировать	имеющихся	абстрактные
		абстрактные	сведений о ТКС	модели циркуляции
		модели циркуляции	формулировать	данных в них
		данных в них	абстрактные	Владеть (или
		Владеть (или	модели циркуляции	Иметь опыт
		Иметь опыт	данных в них	деятельности):
		деятельности):	Владеть (или	Уверенно владеет
		Владеет базовыми	Иметь опыт	навыками
		навыками	деятельности):	формализации и
		формализации и	Владеет основными	математической
		математической	навыками	интерпретации
		интерпретации	формализации и	процессов
		процессов	математической	обработки и
		обработки и	интерпретации	передачи данных в
		передачи данных в	процессов	TKC
		TKC	обработки и	
			передачи данных в	
	TT4 1 2		TKC	
	ПК-1.3	Знать:	Знать:	Знать:
	Формулиру	основные	Требующиеся для	Широкий спектр
	ет целевые	источники	выполнения	источников и
	критерии	информации по	профессиональных	информации по
	для	профессиональной	действий	профессиональной
	оценивания	тематике.	источники	тематике.
	эффективно	Уметь:	информации по	Уметь:
	эффективно	сопоставлять	профессиональной	сопоставлять

1	2	3	4	5
	сти	основные методы и	тематике.	нетиповые методы
	исследуемы	средства	Уметь:	и средства
	х систем	обеспечения	сопоставлять	обеспечения
	A CHCICM	информационной	известные методы	информационной
		безопасности	и средства	безопасности
		потребностям	обеспечения	потребностям
		заказчика и	информационной	заказчика и
		условиям объекта	безопасности	условиям
		невысокой	типовым	конкретного
		сложности.	потребностям	объекта.
		Владеть:	заказчика и	Владеть:
		навыками решения	условиям типового	навыками решения
		базовых задач	объекта.	нестандартных
		комплексного	Владеть:	задач комплексного
		обеспечения	навыками решения	обеспечения
		информационной	стандартных задач	информационной
		безопасности	комплексного	безопасности
		телекоммуникацио	обеспечения	телекоммуникацио
		нных систем.	информационной	нных систем.
			безопасности	
			телекоммуникацио	
			нных систем.	
	ПК-1.4	Знать:	Знать:	Знать:
	Проводит	Принципы	Принципы	Принципы
	эксперимен	организации	организации	организации
	тальные и	элементов	исследований и	исследований
	теоретическ	процессов	процессов	нестандартных
	ие	телекоммуникацио	телекоммуникацио	процессов
		нных систем.	нных систем.	телекоммуникацио
	исследован	Уметь:	Уметь:	нных систем.
	RΝ	реализовывать	Формулировать	Уметь:
	защищённо	задачи,	типовые задачи,	Формулировать и прорабатывать
	сти	планировать и	планировать и	
	телекоммун	проводить	проводить	задачи,
	икационных	исследования в сфере	исследования в сфере	планировать и проводить
	систем и	сфере информационной	информационной	проводить исследования в
	сетей.	безопасности.	безопасности.	сфере
		Владеть:	Владеть:	информационной
		владеет навыками	владеет навыками	безопасности.
		проведения	планирования и	Владеть:
		исследования	проведения	Уверенно владеет
		объектов под	исследования	навыками
		непосредственным	объектов, явлений	планирования и
		руководством.	и процессов	проведения
			телекоммуникацио	исследования
			нных систем.	объектов, явлений
				и процессов
				телекоммуникацио
				нных систем.
ПК-6/	ПК-6.1	Знать:	Знать:	Знать:

1	2	3	4	5
завершаю	Определяет	Основные	Принципы	Принципы
щий	перечень	уязвимости	организации	организации
	информаци	телекоммуникацио	телекоммуникацио	телекоммуникацио
	И,	нных систем.	нных систем и их	нных систем и их
	подлежаще	Уметь:	основные	уязвимости, в том
	й защите	Формулировать	уязвимости.	числе нетиповые.
		отдельные	Уметь:	Уметь:
		требования к	Формулировать	Прорабатывать и
		телекоммуникацио	технические	детализировать
		нным системам и	требования к	технические
		мерам по	телекоммуникацио	требования к
		предотвращению	нным системам и	телекоммуникацио
		уязвимостей.	мерам по	нным системам и
		Владеть:	предотвращению	мерам по
		навыками создания	уязвимостей.	предотвращению
		примитивных	Владеть:	уязвимостей.
		моделей угроз и	навыками создания	Владеть:
		моделей	стандартных	навыками создания
		злоумышленника	моделей угроз и	сложных и
		для	моделей	нетиповых моделей
		телекоммуникацио	злоумышленника	угроз и моделей
		нных систем и	для	злоумышленника
		устройств.	телекоммуникацио	для
			нных систем и	телекоммуникацио
			устройств.	нных систем и
				устройств.
	ПК-6.2	Знать:	Знать:	Знать:
	Определяет	Фрагменты и	Основные законы,	Совокупность
	требуемый	отдельные законов,	технологии,	законов,
	уровень	технологий,	правила, приемы	технологий,
	защищённо	правил, приемов	обработки	правил, приемов
	сти	обработки	исследования	обработки
	информаци	исследования	уровня	исследования
	И,	уровня	защищенности	уровня
	циркулиру	защищенности	объектов	защищенности
	ющей в	объектов	информатизации.	объектов
		1	Уметь:	информатизации.
	телекоммун	информатизации.	уметь:	информатизации.
	телекоммун икационной	информатизации. Уметь:	подготовить отчет	Уметь:
	·		подготовить отчет по результатам	Уметь: подготовить
	икационной	Уметь:	подготовить отчет по результатам обследования	Уметь:
	икационной	Уметь: подготовить	подготовить отчет по результатам обследования объекта.	Уметь: подготовить развернутый отчет по результатам
	икационной	Уметь: подготовить отдельные части отчета по результатам	подготовить отчет по результатам обследования	Уметь: подготовить развернутый отчет по результатам обследования
	икационной	Уметь: подготовить отдельные части отчета по результатам обследования	подготовить отчет по результатам обследования объекта.	Уметь: подготовить развернутый отчет по результатам обследования объекта.
	икационной	Уметь: подготовить отдельные части отчета по результатам обследования объекта.	подготовить отчет по результатам обследования объекта. Владеть: навыками подготовки	Уметь: подготовить развернутый отчет по результатам обследования объекта. Владеть:
	икационной	Уметь: подготовить отдельные части отчета по результатам обследования	подготовить отчет по результатам обследования объекта. Владеть: навыками подготовки аттестационных	Уметь: подготовить развернутый отчет по результатам обследования объекта.
	икационной	Уметь: подготовить отдельные части отчета по результатам обследования объекта. Владеть: навыками	подготовить отчет по результатам обследования объекта. Владеть: навыками подготовки аттестационных документов на	Уметь: подготовить развернутый отчет по результатам обследования объекта. Владеть: уверенными навыками
	икационной	Уметь: подготовить отдельные части отчета по результатам обследования объекта. Владеть: навыками подготовки	подготовить отчет по результатам обследования объекта. Владеть: навыками подготовки аттестационных документов на предмет	Уметь: подготовить развернутый отчет по результатам обследования объекта. Владеть: уверенными навыками подготовки
	икационной	Уметь: подготовить отдельные части отчета по результатам обследования объекта. Владеть: навыками подготовки отдельных	подготовить отчет по результатам обследования объекта. Владеть: навыками подготовки аттестационных документов на предмет соответствия	уметь: подготовить развернутый отчет по результатам обследования объекта. Владеть: уверенными навыками подготовки аттестационных
	икационной	Уметь: подготовить отдельные части отчета по результатам обследования объекта. Владеть: навыками подготовки отдельных аттестационных	подготовить отчет по результатам обследования объекта. Владеть: навыками подготовки аттестационных документов на предмет соответствия объекта	уметь: подготовить развернутый отчет по результатам обследования объекта. Владеть: уверенными навыками подготовки аттестационных документов на
	икационной	Уметь: подготовить отдельные части отчета по результатам обследования объекта. Владеть: навыками подготовки отдельных	подготовить отчет по результатам обследования объекта. Владеть: навыками подготовки аттестационных документов на предмет соответствия	уметь: подготовить развернутый отчет по результатам обследования объекта. Владеть: уверенными навыками подготовки аттестационных

1	2	3	4	5
		соответствия объекта требованиям по информационной безопасности.	безопасности.	объекта требованиям по информационной безопасности.
	ПК-6.3	Знать:	Знать:	Знать:
	Определяет	Назначение	Инструментальные	Полный спектр
	меры для	инструментальных	средства	инструментальных
	защиты в	средств	обеспечения	средств
	информаци	обеспечения	защиты	обеспечения
	ИВ	защиты	информации	защиты
	телекоммун	информации	телекоммуникацио	информации
	икационных	телекоммуникацио	нных систем.	телекоммуникацио
	системах и	нных систем.	Уметь:	нных систем.
	сетях	Уметь:	Осуществлять	Уметь:
		Выделять	выбор средств	Осуществлять
		требуемые	обеспечения	рациональный
		характеристики средств	информационной безопасности	выбор средств обеспечения
		обеспечения	телекоммуникацио	информационной
		информационной	нных систем.	безопасности
		безопасности	Владеть:	телекоммуникацио
		телекоммуникацио	Навыками	нных систем.
		нных систем.	эксплуатации	Владеть:
		Владеть:	телекоммуникацио	Уверенными
		Базовыми	нных приборов и	навыками
		навыками	средств защиты	эксплуатации
		эксплуатации	информации.	телекоммуникацио
		телекоммуникацио		нных приборов и
		нных приборов и		средств защиты
		средств защиты		информации.
		информации.		
ПК-7/	ПК-7.1	Знать: структуру и	<i>Знать:</i> структуру и	Знать: структуру и
завершаю	Разрабатыва	содержание	содержание	содержание
щий	ет	технических	технических	технических
	технические	заданий на	заданий на	заданий на
	задания на	проведение	проведение	проведение работ
	модернизац	отдельных этапов	основных этапов	по обеспечению
	ию систем	работ по	работ по	информационной
	защиты информаци	обеспечению информационной	обеспечению информационной	безопасности Уметь:
		безопасности	безопасности	формулировать
	И	Уметь:	Уметь:	задачи и цели
		формулировать	формулировать	модернизации
		последовательност	задачи и цели	системы
		и задач по	модернизации	обеспечения
		модернизации	системы	информационной
		'' 1		
1		системы	обеспечения	безопасности и

1	2	3	4	5
		информационной	безопасности	достижения
		безопасности	Владеть (или	Владеть (или
		Владеть (или	Иметь опыт	Иметь опыт
		Иметь опыт	деятельности):	деятельности):
		деятельности):	формулирования	формулирования
		формулирования	заданий для	проработанных
		этапов работ по	обеспечения	заданий для
		обеспечению	информационной	обеспечения
		информационной	безопасности	информационной
		безопасности		безопасности
	ПК-7.2	Знать:	Знать: основные	Знать: правила,
	Формирует	номенклатуру	правила	регламенты и
	документы	правил выполнения	выполнения работ	порядок
	для	работ по	по обеспечению	выполнения работ
	обосновани	обеспечению	информационной	по обеспечению
	Я	информационной	безопасности	информационной
	разработки	безопасности	Уметь:	безопасности
	И	Уметь: с	документально	Уметь:
	модернизац	недостатками	описывать	документально и в
	ии систем	документально	основные	полном объёме
	защиты	описывать	применяемые для	описывать
	информаци	применяемые для	обеспечения	применяемые для
	И	обеспечения	безопасности ТКС	обеспечения
		безопасности ТКС	технологии	безопасности ТКС
		технологии	Владеть (или	технологии
		Владеть (или	Иметь опыт	Владеть (или
		Иметь опыт	деятельности):	Иметь опыт
		деятельности):	разработки и	деятельности):
		проведения работ	модернизации	разработки и
		по разработке и	систем защиты	модернизации
		модернизации	информации	систем защиты
		систем защиты		информации для
		информации		достижения
				целевых
				показателей
				функционирования
	ПК-7.3	Знать: структуру	Знать: принципы и	Знать:
	Разрабатыва	моделей угроз и	структуру моделей	фундаментальные
	ет модели	моделей	угроз и моделей	принципы и
	угроз и	нарушителя	нарушителя	структуру моделей
	модели	Уметь:	Уметь: соотносить	угроз и моделей
	нарушителе	формулировать	уязвимости в	нарушителя
	й	возможности	телекоммуникацио	<i>Уметь:</i> соотносить
		злоумышленников	нных системах	уязвимости в
		Владеть (или	возможностям	сложных и
		Иметь опыт	злоумышленников	нетиповых
		деятельности):	Владеть (или	телекоммуникацио
		сопоставления	Иметь опыт	нных системах
		категорий	деятельности):	ВОЗМОЖНОСТЯМ
		злоумышленников	определения	злоумышленников
		характеристикам	категорий	Владеть (или

1	2	3	4	5
		телекоммуникацио нных систем	злоумышленников исходя из характеристик телекоммуникацио нных систем	Иметь опыт деятельности): формирования оригинальных методик определения категорий злоумышленников исходя из характеристик телекоммуникацио нных систем
	ПК-7.4	Знать:	Знать: структуру и	Знать: полную
	Готовит проекты нормативны х и методическ их материалов, регламенти рующих выполнение работ по защите информаци и	номенклатуру нормативных документов по обеспечению информационной безопасности Уметь: сопоставлять этапы работ по обеспечению информационной безопасности целям организации Владеть (или Иметь опыт деятельности): проведения работ по информационной безопасности	состав основных нормативных документов по обеспечению информационной безопасности Уметь: определять этапы работ по обеспечению информационной безопасности Владеть (или Иметь опыт деятельности): проведения и документального обеспечения работ по информационной безопасности	структуру и состав нормативных документов по обеспечению информационной безопасности Уметь: анализировать имеющиеся требования нормативных документов и формулировать положения по проведению работ по обеспечению информационной безопасности Владеть (или Иметь опыт деятельности): проведения и точного документального обеспечения работ по информационной по информационной обеспечения работ по информационной
ПК-8/	ПК-8.1	<i>Знать:</i> порядок	<i>Знать:</i> порядок	безопасности Знать: методику
завершаю щий	Управляет работой специалист ов по созданию и эксплуатаци и средств защиты	действий специалистов по эксплуатации средств защиты информации в телекоммуникацио нных системах и сетях	действий специалистов по созданию и эксплуатации средств защиты информации в телекоммуникацио нных системах и	определения порядка действий специалистов по созданию и эксплуатации средств защиты информации в телекоммуникацио
	информаци	Уметь: ставить	сетях	нных системах и

1	2	3	4	5
1	и в телекоммун икационных системах и сетях	задачи отдельным исполнителям и эксплуатации средств защиты информации в телекоммуникацио нных системах и сетях Владеть (или Иметь опыт деятельности): эксплуатации средств защиты информации в телекоммуникацио нных системах и сетях	Уметь: ставить задачи отдельным исполнителям при создании и эксплуатации средств защиты информации в телекоммуникацио нных системах и сетях Владеть (или Иметь опыт деятельности): созданию и эксплуатации средств защиты информации в телекоммуникацио нных системах и сетях	сетях Уметь: ставить задачи всем исполнителям при создании и эксплуатации средств защиты информации в телекоммуникацио нных системах и сетях Владеть (или Иметь опыт деятельности): создания и эксплуатации сложных средств защиты информации в телекоммуникацио
			сетях	телекоммуникацио нных системах и сетях
	ПК-8.2	<i>Знать:</i> перечень	<i>Знать:</i> перечень	Знать: методики
	Формирует комплекс мер (принципов, правил, процедур, практическ их приемов, методов, средств) для защиты в телекоммун икационных	угроз, на нейтрализацию которых направлены отдельные меры по защите информации <i>Уметь:</i> проводить отдельные мероприятия по обеспечению информационной безопасности в	угроз, на нейтрализацию которых направлена та или иная мера по защите информации Уметь: последовательно проводить отдельные мероприятия по обеспечению	определения угроз, на нейтрализацию которых направлена та или иная мера по защите информации Уметь: объединять отдельные мероприятия по обеспечению информационной безопасности в
	системах и сетях информаци и ограниченн ого доступа	логически структурированные последовательност и Владеть (или Иметь опыт деятельности): использования отдельных технологий обеспечения информационной безопасности в ТКС	информационной безопасности в логически структурированные последовательност и Владеть (или Иметь опыт деятельности): использования типовых технологий обеспечения информационной безопасности в	логически структурированные последовательност и Владеть (или Иметь опыт деятельности): использования разнообразных технологий обеспечения информационной безопасности в ТКС

1	2	3	4	5
			TKC	
	ПК-8.3	Знать:	Знать:	Знать: правила и
	Управляет	административный	административный	административный
	процессом	регламент	регламент	регламент
	разработки	проведения работ	проведения работ	проведения работ
	моделей	по обеспечению	по обеспечению	по обеспечению
	угроз и	информационной	информационной	информационной
	моделей	безопасности	безопасности	безопасности
	нарушителя	Уметь: при	Уметь: принимать	Уметь: принимать
	безопасност	поддержке	управленческие	и обосновывать
	И	принимать	решения при	управленческие
	компьютерн	управленческие	проведении работ	решения при
	ых систем	решения при	по обеспечению	проведении работ
		проведении работ	информационной	по обеспечению
		по обеспечению	безопасности	информационной
		информационной	Владеть (или	безопасности
		безопасности	Иметь опыт	Владеть (или
		Владеть (или	деятельности):	Иметь опыт
		Иметь опыт	разработки	деятельности):
		деятельности):	моделей угроз и	разработки
		разработки	моделей	оригинальных
		элементов моделей	нарушителя	моделей угроз и
		угроз и моделей	безопасности для	моделей
		нарушителя	типовых	нарушителя
		безопасности	компьютерных	безопасности
		компьютерных	систем	компьютерных
		систем		систем
	ПК-8.4	Знать:	<i>Знать:</i> основные	Знать: все
	Разрабатыва	номенклатуру	этапы жизненного	возможные этапы
	ет	этапов жизненного	цикла ТКС и	жизненного цикла
	организаци	цикла ТКС и	регламентные	ТКС и
	онно-	регламентные	мероприятия на	регламентные
	распорядите	мероприятия на	каждом из них	мероприятия на
	льные	каждом из них	<i>Уметь:</i> выполнять	каждом из них
	документы,	<i>Уметь:</i> выполнять	небольшие	<i>Уметь:</i> выполнять
	регламенти	отдельные	последовательност	связанные
	рующие	действия по	и отдельных	последовательност
	порядок	обеспечению	действий по	и действий по
	эксплуатаци	информационной	обеспечению	обеспечению
	И	безопасности	информационной	информационной
	телекоммун	телекоммуникацио	безопасности	безопасности
	икационных	нных систем	телекоммуникацио	телекоммуникацио
	систем и	Владеть (или	нных систем	нных систем
	сетей	Иметь опыт	Владеть (или	Владеть (или
		деятельности):	Иметь опыт	Иметь опыт
		систематизации	деятельности):	деятельности):
		отдельных	систематизации	систематизации
		действий по	последовательност	сложных
		обеспечению	и действий по	последовательносте
		информационной	обеспечению	й действий по
		безопасности	информационной	обеспечению

1	2	3	4	5
		телекоммуникацио нных систем	безопасности телекоммуникацио нных систем	информационной безопасности телекоммуникацио нных систем
	ПК 8.5 Определяет действия сотруднико в при проведении мероприяти й по информаци онной безопасност и	Знать: Организацию судебных, правоприменительных и правоохранительны х органов Уметь: определять перечень действий для проведения анализа ИБ Владеть (или Иметь опыт деятельности): Навыками работы с нормативноправовыми документами	Знать: правовые нормы действующего законодательства, регулирующие отношения в различных сферах жизнедеятельности. Уметь: работать с нормативными документами регуляторов в области информационной безопасности Владеть (или Иметь опыт деятельности): работой с методической литературой и вырабатывать управленческие решения в области информационной безопасности;	Знать: основные положения и нормы конституционного, гражданского, семейного, трудового, административного и уголовного права. Уметь: определять актуальные вопросы защиты информации в соответствии с уровнем уязвимости Владеть (или Иметь опыт деятельности): Навыками применения нормативных правовых документов в конкретных практических ситуациях
ПК-9/ завершаю щий	ПК-9.1 Выявляет сбои и отказы устройств и программ	Знать: отдельные признаки возникновения сбоев и отказов при эксплуатации ТКС Уметь: под руководством в процессе эксплуатации фиксировать режимы работы ТКС, отличные от штатных Владеть (или Иметь опыт деятельности): обнаружения части сбоев и отказов реальных ТКС	Знать: основные признаки возникновения сбоев и отказов при эксплуатации ТКС Уметь: в процессе эксплуатации фиксировать режимы работы ТКС, отличные от штатных Владеть (или Иметь опыт деятельности): обнаружения сбоев и отказов типовых ТКС	Знать: различные, в том числе нетиповые признаки возникновения сбоев и отказов при эксплуатации ТКС Уметь: в процессе эксплуатации выявлять и фиксировать режимы работы ТКС, отличные от штатных Владеть (или Иметь опыт деятельности): обнаружения сбоев и отказов сложных ТКС

ПК-9	0.2 3	•		
Rocc		нать: знать	<i>Знать:</i> порядок	<i>Знать:</i> знать цели
Bocc	танавл н	оменклатуру	проведения	и задачи
ивает	-	егламентных	регламентных	регламентных
рабоз	госпосо ра	абот по	работ по	работ по
бнос		осстановлению	восстановлению	восстановлению
систе	ем ра	аботоспособности	работоспособности	работоспособности
после	е сбоев у	стройств и	устройств и	устройств и
и отк	азов п	рограмм	программ	программ
устро	ойств и У	Уметь: выполнять	Уметь: оперативно	Уметь: выполнять
прог	рамм р	егламентные	выполнять	точно и оперативно
	p	аботы по	регламентные	требуемые работы
	В	осстановлению	работы по	по восстановлению
	p	аботоспособности	восстановлению	работоспособности
	y	стройств и	работоспособности	устройств и
	П	рограмм	устройств и	программ
		Владеть (или	программ	Владеть (или
		Іметь опыт	Владеть (или	Иметь опыт
	d	еятельности):	Иметь опыт	деятельности):
		ксплуатации	деятельности):	эксплуатации
		тдельных	эксплуатации	программного и
		лементов	программного и	аппаратного
	П	рограммного и	аппаратного	обеспечения ТКС в
		ппаратного	обеспечения ТКС	различных
		беспечения ТКС		режимах работы
ПК-9	0.3 3	нать: назначение	<i>Знать:</i> назначение	<i>Знать:</i> назначение
Форм	иулиру и		и классификацию	и классификацию
_		рограммно-	программно-	программно-
дейс	-	ппаратных средств	аппаратных средств	аппаратных средств
для		ГКС; технические	ТКС; особенности	ТКС; особенности
Восст	гановле х	арактеристики и	функционирования	функционирования
ния	п	равила	ТКС; систем	TKC;
после	едстви э	ксплуатации	обнаружения	классификацию
й сбо	ев и С	редств	сетевых атак,	программных и
отказ	вов в	осстановления	антивирусного ПО;	аппаратных средств
	п	оследствий сбоев	технические	анализа
	и	готказов.	характеристики и	защищённости
		_	правила	ТКС, систем
		меть: провести	эксплуатации	обнаружения
		астройку ПО и	средств	сетевых атак,
	0	борудования ТКС.	восстановления	антивирусного ПО;
	_D	Pradami.	последствий сбоев	технические
		Владеть:	и отказов.	характеристики и
		авыками		правила
		астройки,	Уметь: проводить	эксплуатации
		нтивирусного ПО.	мониторинг	средств
			безопасности АС;	восстановления
			провести настройку	последствий сбоев
			ПО и оборудования	и отказов.
			TKC.	
			Ruadami	Уметь: проводить
			Владеть:	мониторинг

1 2	3	4	5
		навыками настройки программных и аппаратных средств анализа защищённости ТКС, антивирусного ПО.	безопасности АС; обнаруживать уязвимые места в функционировании ПО и оборудования ТКС; провести настройку ПО и оборудования ТКС.
			Владеть: навыками настройки программных и аппаратных средств анализа защищённости ТКС, систем обнаружения сетевых атак, антивирусного ПО.
ПК-9.4	Знать:	<i>Знать:</i> основные	Знать: методику
Регистр		признаки	выявления
т сообще	ошибок в сетевых		признаков
об оши	" +	ошибок в сетевых устройствах и	возникновения ошибок в сетевых
в сетевн	1 '	операционных	устройствах и
устройс			операционных
и	эксплуатации	Уметь: в процессе	системах
операци		эксплуатации	Уметь: в процессе
ых сист		фиксировать	эксплуатации
	сетевых устройств		обнаруживать и
	и операционных	сетевых устройств	фиксировать
	систем, отличные	* *	режимы работы
	от штатных	систем, отличные	сетевых устройств
	Владеть (или	от штатных	и операционных
	Иметь опыт	Владеть (или	систем, отличные
	деятельности):	Иметь опыт	от штатных
	навыками	деятельности):	Владеть (или
	протоколирования отдельных сбоев и		Иметь опыт
	отдельных сооев в отказов реальных	1	<i>деятельности):</i> навыками
	сетевых устройст		обнаружения и
	и операционных	устройств и	протоколирования
	систем	операционных	сбоев и отказов
		систем	реальных сетевых
			устройств и
			операционных
			систем
ПК-9.5	<i>Знать:</i> структуру	Знать: структуру и	<i>Знать:</i> методику
Формир		содержание	формирования
отчёты	по информационной	журналов аудита	журналов аудита

1	2	3	4	5
	результатам	безопасности	информационной	информационной
	работ	Уметь: под	безопасности	безопасности
	системы	руководством	Уметь:	Уметь: выбирать и
	мониторинг	использовать	использовать	использовать
	a	технические	технические	технические
		средства ведения	средства ведения	средства ведения
		журналов аудита	журналов аудита	журналов аудита
		информационной	информационной	информационной
		безопасности	безопасности	безопасности
		Владеть (или	Владеть (или	Владеть (или
		Иметь опыт	Иметь опыт	Иметь опыт
		деятельности):	деятельности):	деятельности):
		навыками	навыками работы с	навыками анализа
		формирования	журналами аудита	журналов аудита
		журналов аудита	информационной	информационной
		информационной	безопасности	безопасности
		безопасности		
ПК-10/	ПК-10.1	Знать:	<i>Знать:</i> основные	Знать: методику
завершаю	Проверяет	номенклатуру	признаки	выявления
щий	корректност	ошибок в	возникновения	признаков
	ь работы	программных	ошибок в в	возникновения
	программн	компонентах	программных	ошибок в
	ЫХ	телекоммуникацио	компонентах	программных
	компонент	нной системы	телекоммуникацио	компонентах
	телекоммун	Уметь: в процессе	нной системы	телекоммуникацио
	икационной	эксплуатации	Уметь: в процессе	нной системы
	системы	фиксировать	эксплуатации	Уметь: в процессе
		режимы работы в	фиксировать	эксплуатации
		программных	режимы работы в	обнаруживать и
		компонентах	программных	фиксировать
		телекоммуникацио	компонентах	режимы работы в
		нной системы,	телекоммуникацио	программных
		отличные от	нной системы	компонент
		штатных	Владеть (или	телекоммуникацио
		Владеть (или	Иметь опыт	нной системы
		Иметь опыт	деятельности):	Владеть (или
		деятельности):	навыками	Иметь опыт
		навыками	протоколирования сбоев и отказов в	<i>деятельности):</i> навыками
		протоколирования отдельных сбоев и		
		отдельных сооев и отказов в	программных компонентах	обнаружения и протоколирования
			телекоммуникацио	протоколирования сбоев и отказов в
		программных компонентах	нной системы	программных
		телекоммуникацио	IIIION CHCICIOIDI	компонентах
		нной системы		телекоммуникацио
		IIIIOII ONO I ONIDI		нной системы
	ПК-10.2	Знать:	Знать:	Знать:
	Определяет	Понятия профиля	Профили защиты	Методику
	соответстви	защиты	инструментальные	формирования
	е текущего	инструментальные	средства	профилей защиты
	функционал	средства	обеспечения	инструментальных
L	TJ	1 -1-0		1

1	2	3	4	5
	а системы требования м профилей защиты	обеспечения защиты информации телекоммуникацио нных систем. Уметь: Использовать средства реализации профилей защиты. Владеть: Навыками работы с элемнтарными профилями защиты.	защиты информации телекоммуникацио нных систем. Уметь: Осуществлять выбор средств реализации профилей защиты. Владеть: Навыками работы с профилями защиты.	средств обеспечения защиты информации телекоммуникацио нных систем. Уметь: Осуществлять рациональный выбор эффективных средств реализации профилей защиты. Владеть: Навыками работы со сложными и многоуровневыми профилями защиты.
	ПК-10.3 Формирует систематизи рованные политики информаци онной безопасност и	Знать: отдельные этапы жизненного цикла ТКС и регламентные мероприятия на каждом из них Уметь: выполнять действия по обеспечению информационной безопасности телекоммуникацио нных систем Владеть (или Иметь опыт действие по обеспечению информационной безопасности телекоммуникации отдельных действие по обеспечению информационной безопасности телекоммуникацио нных систем	Знать: основные этапы жизненного цикла ТКС и регламентные мероприятия на каждом из них Уметь: выполнять последовательност и действий по обеспечению информационной безопасности телекоммуникацио нных систем Владеть (или Иметь опыт действие по обеспечению информационной безопасности телекоммуникации действие по обеспечению информационной безопасности телекоммуникацио нных систем	Знать: все этапы жизненного цикла ТКС и регламентные мероприятия на каждом из них Уметь: выполнять связанные последовательност и действий по обеспечению информационной безопасности телекоммуникацио нных систем Владеть (или Иметь опыт действий по обеспечению информационной обеспечению информационной обеспечению и действий по обеспечению информационной безопасности телекоммуникацио нных систем
	ПК-10.4 Разрабатыва ет профили	Знать: Структуру и содержание отдельных	Знать: Структуру и содержание профилей заданий	Знать: Методику формирования профилей заданий
	заданий по	профилей заданий	по безопасности	по безопасности

1	2	3	4	5
	безопасност	по безопасности	для оборудования	для оборудования
	и для	для оборудования	телекоммуникацио	телекоммуникацио
	оборудован	телекоммуникацио	нных систем в	нных систем в
	ия	нных систем в	защищённом	защищённом
	телекоммун	защищённом	исполнении	исполнении
	икационных	исполнении	Уметь:	Уметь:
	систем в	Уметь:	структурировать	структурировать
	защищённо	структурировать	отдельные	сложные
	M	небольшие	процедуры и	последовательност
	исполнении	последовательност	регламентные	и процедур и
		и процедур и	работы в единые	регламентных
		регламентных	систематические	работ в единые
		работ в единые	профили	систематические
		систематические	безопасности	профили
		профили	Владеть (или	безопасности
		безопасности	Иметь опыт	Владеть (или
		Владеть (или	деятельности):	Иметь опыт
		Иметь опыт	навыками	деятельности):
		деятельности):	эксплуатации	уверенными
		навыками	оборудования	навыками
		эксплуатации	телекоммуникацио	эксплуатации
		оборудования	нных систем в	оборудования
		телекоммуникацио	защищённом	телекоммуникацио
		нных систем	исполнении	нных систем в
				защищённом
THC 11/	THC 11 1	2		исполнении
ПК-11/	ПК-11.1	Знать:	Знать:	Знать:
завершаю щий	Определяет	номенклатуру	характеристики	особенности
ЩШ	действия по	этапов жизненного цикла ТКС	различных этапов	различных этапов
	обеспечени	'	жизненного цикла ТКС	жизненного цикла ТКС
	ю информаци	Уметь: исходя их ограниченного	Уметь: исходя их	Уметь: исходя их
	онной	перечня угроз	имеющегося	обширного перечня
	безопасност	реализовывать	перечня угроз	угроз
	и на	технологии	реализовывать	реализовывать
	различных	обеспечения	технологии	технологии
	этапах	информационной	обеспечения	обеспечения
	жизненного	безопасности	информационной	информационной
	цикла	Владеть (или	безопасности	безопасности
	телекоммун	Иметь опыт	Владеть (или	Владеть (или
	икационной	деятельности):	Иметь опыт	Иметь опыт
	системы	эксплуатации ТКС	деятельности):	деятельности):
		на отдельных	эксплуатации TKC	эксплуатации TKC
		этапах жизненного	на основных этапах	на различных
		цикла	жизненного цикла	этапах жизненного
				цикла
	ПК-11.2	<i>Знать:</i> перечень	<i>Знать:</i> структуру	Знать: структуру и
	Выбирает	реализуемых	реализуемых	особенности
1	HODOMOM	телекоммуникацио	телекоммуникацио	реализуемых
	перечень			1 = -
	реализуемы	нной системой технологий для	нной системой технологий для	телекоммуникацио нной системой

телекоммун икационной системой требований по информационной системой информационной безопасности удовлетворения требований по информационной безопасности удовлетворения требований по информационной безопасности уществующим в владеть (или информационной безопасности уществующим в владеть (или информационной безопасности результативности применения штатных средств обеспечения информационной безопасности информационной б	1	2	3	4	5
пия удовдетворе ния технологии уметь: соотносить основные технологии информационной безопасности информационной б					· ·
технологий для			-	_	
удовлетворе ния требований по обезопасности информационной обезопасности и информационной обезопасности информационной обезопасности и информационной обеспечения информационной обезопасности и информационной обезопасности и информационной обезопасности и информационной обезопас		системой	информационной	информационной	требований по
удовлетворе ния требований по технологии технологии информационной безопасности информационной безопасности информационной безопасности информационной безопасности информационной безопасности и информационной безопасности информационной информационной информационной информационной безопасности информационной информационной информационной безопасности информацио		технологий	безопасности	безопасности	информационной
технологии информационной безопасности существующим в тКС уязвимостям владеть (или информационной безопасности ин		для	<i>Уметь:</i> соотносить	Уметь: соотносить	безопасности
требований по информационной безопасности информации онной безопасности и информации онной безопасности и информационной безопасности информационно		удовлетворе	отдельные	основные	Уметь: соотносить
безопасности существующим в ТКС узявимостям Владеть (или Иметь опыт деятельностии): реализации реализации реализации информационной безопасности ПК-11.3 Знать: молчественные количественные количественные количественные количественные количественные количественные количественные количествения штатных средств обеспечения информационной безопасности взядьтивности применения штатных средств обеспечения информационной безопасности взядь обеспечения информационной безопасности и взядь обеспечения информационной безопасности		кин	технологии	технологии	технологии
тиформации пинормации пинор		требований	информационной	информационной	информационной
онной безопасност и ТКС уязвимостям Владеть (или Иметь опыт деятельностии): реализации безопасности ТКТ уязвимостям Владеть (или Иметь опыт деятельностии): реализации реализации реализации информационной безопасности ТК-11.3 Знать: шкалы результативности применения штатных обеспечения информационной безопасности ТК-11.3 Оценивает результативности применения штатных обеспечения информационной безопасности ТКТ уязвимостям Владеть (или Иметь опыт деятельностии): реализации реализации стехнологий информационной безопасности информационной безопасности информационной безопасности уметь: уметь: формулировать количественные количественные количественные количественные методы обеспечения информационной безопасности инф		ПО	безопасности	безопасности	безопасности
безопасност и Владеть (или Иметь опыт деятельности реализации базовых технологий информационной безопасности результатт применения птатных средств информаци онной безопасности безопасности безопасности применения птатных средств обеспечения информационной безопасности безопасности безопасности применения птатных средств обеспечения информационной безопасности применения птатных средств обеспечения информационной безопасности применения птатных средств обеспечения информационной безопасности применения птатных средств обеспечения информационной безопасности применения птатных средств обеспечения информационной безопасности Владеть (или Иметь опыт деяться не безопасности применения прадеть (или Иметь опыт деяться технологий деятьсногогий деяться технологий деяться технологий деяться технологий деятьсности применения п		информаци	существующим в	существующим в	существующим в
Иметь опыт феятельности): реализации базовых соновных технологий информационной безопасности информационной безопасности применения интатных средств информационной безопасности информационной безопасности информационной безопасности информационной безопасности информационной обеспечения интатных средств обеспечения интатных средств обеспечения информационной безопасности информационной бе		онной	ТКС уязвимостям	ТКС уязвимостям	ТКС уязвимостям
реализации стека технологий информационной безопасности ПК-11.3 Оценивает результат применения птатных средств обеспечения информационной безопасности я уметь: информационной безопасности уметь: использовать формулировать количественные количественные количественные количественные количественные количественные критерии результативности применения примененыя птатных средств обеспечении информационной безопасности информационной безопасности информационной безопасности информационной безопасности врадьенные критерии результативности применения применен		безопасност	Владеть (или	Владеть (или	Владеть (или
реализации основных технологий информационной безопасности ПК-11.3 Оценивает результат применения информационной безопасности информационной		И	Иметь опыт	Иметь опыт	Иметь опыт
основных технологий информационной безопасности безопасности безопасности применения применения информационной безопасности применения информационной безопасности применения применения применения информационной безопасности применения примен			деятельности):	деятельности):	деятельности):
технологий информационной безопасности ПК-11.3 Оценивает результат применения применения штатных средств обеспечения онной безопасности и информационной безопасности и результативности применения интатных средств обеспечения информационной безопасности и результативности применения информационной безопасности информ			реализации	реализации	реализации стека
ПК-11.3 Знать: шкалы обеспечения штатных средств информационной обеспечения информационной обеспе				основных	_
ПК-11.3 Знать: шкалы обеспечения штатных средств информационной обеспечения информационной обеспе			технологий	технологий	информационной
ПК-11.3 Оценивает результативности применения применения применения информационной безопасности информационной б			информационной	информационной	
Оценивает результати применения информационной безопасности уметь: формулировать количественные количественные количественные количественные количественные количественные количественные количественные количественные применения при					
Оценивает результат применения информационной безопасности уметь: формулировать количественные количественные критерии результативности применения примен		ПК-11.3	<i>Знать:</i> шкалы	<i>Знать:</i> критерии	Знать: методику
применения штатных средств обеспечения обеспечения информационной безопасности информационной безопасности информационной безопасности информационной обеспечения информационной обесп		Оценивает	результативности	результативности	оценки
обеспечения информационной безопасности уметь: информации онной количественные критерии результативности применения информационной безопасности информационной безопасности информационной безопасности информационной безопасности информационной информационной безопасности информационной безопасности информационной информационной безопасности информационной безопасности информационной безопасности информационной информационной безопасности информац		результат	применения	применения	результативности
средств обеспечени я информационной безопасности уметь: информаци онной безопасности уметь: использовать количественные количественные количественные критерии результативности применения штатных средств обеспечения информационной безопасности Владеть (или Иметь опыт деятельности): навыками применения штатных средств обеспечения информационной безопасности Владеть (или Иметь опыт деятельности): навыками применения штатных средств обеспечения информационной безопасности Владеть (или Иметь опыт деятельности): навыками оценки применения штатных средств обеспечения информационной безопасности штатных средств обеспечения информационной безопасности применения применения применения применения применения информационной безопасности информационной безопасн		применения	штатных средств	штатных средств	применения
обеспечени я информаци онной количественные количественные количественные критерии результативности применения штатных средств обеспечения информационной безопасности Владеть (или Иметь опыт деятельности): навыками применения штатных средств обеспечения информационной безопасности Владеть (или Иметь опыт деятельности): навыками применения штатных средств обеспечения информационной безопасности Владеть (или Иметь опыт деятельности): навыками применения штатных средств обеспечения информационной безопасности применения применения применения применения применения применения информационной безопасности информацион		штатных	обеспечения	обеспечения	штатных средств
я информаци онной количественные критерии результативности применения применения информационной безопасности Владеть (или Иметь опыт деятельностии): навыками применения применения применения применения применения информационной безопасности Владеть (или Иметь опыт деятельности): навыками применения применения применения информационной безопасности вавиками применения применения применения применения применения информационной безопасности Владеть (или Иметь опыт деятельности): навыками применения примень обеспечения информационной безопасности применения применения применения применения примень обеспечения информационной безопасности применения применения применения применения информационной безопасности применения п		средств	информационной	информационной	обеспечения
информаци онной количественные критерии результативности применения штатных средств обеспечения информационной безопасности Владеть (или Иметь опыт деятельности): навыками применения применения применения применения применения информационной безопасности вывыками применения применения применения информационной безопасности владеть (или Иметь опыт деятельности): навыками применения		обеспечени	безопасности	безопасности	информационной
онной безопасност и результативности применения штатных средств обеспечения информационной безопасности Владеть (или Иметь опыт деятельности): навыками применения штатных средств обеспечения информационной безопасности вавыками применения штатных средств обеспечения информационной безопасности вавыками применения штатных средств обеспечения информационной безопасности применения применения информационной безопасности вавыками оценки применения информационной безопасности применения применения применения информационной безопасности информационной информаци		Я	Уметь:	Уметь:	безопасности
безопасност и результативности применения штатных средств обеспечения информационной безопасности и применения штатных средств обеспечения информационной безопасности и применения информационной безопасности и применения информационной безопасности и информационной обеспечения информационной безопасности информационной информационной информационной		информаци	использовать	формулировать	Уметь:
и результативности применения информационной безопасности владеть (или Иметь опыт деятельности): навыками применения примень обеспечения применения применения примень обеспечения примень обеспечения применения применения примень обеспечения примень обеспечения примень обеспечения применения примень обеспечения обеспечения примень обеспечения обе		онной	количественные	количественные	формулировать
применения обеспечения обеспечения информационной безопасности информационной безопасности информироваными применения применения применения применения применения применения применения применения применения обеспечения информационной безопасности информационной информационной информационной информационной информационной информационной информационной информационной ин		безопасност	критерии	критерии	методы оценки
птатных средств обеспечения информационной безопасности владеть (или иметь опыт деятельности): навыками применения информационной обеспечения информационной обеспечения информационной обеспечения информационной обезопасности владеть (или иметь опыт деятельности): навыками применения применения интатных средств обеспечения информационной обеспечения информационной обеспечения информационной обезопасности информационной		И	результативности	результативности	результативности
обеспечения информационной безопасности владеть (или иметь опыт деятельности): навыками применения информационной обеспечения ин			применения	применения	применения
безопасности Владеть (или Иметь опыт деятельности): навыками применения применения информационной безопасности Владеть (или Иметь опыт деятельности): навыками оценки применения применения информационной безопасности ПК-11.4 Знать: базовые Формулиру безопасности безопасности Владеть (или Иметь опыт деятельности): навыками оценки праультативности применения праультативности применения п			-	_	_
безопасности Владеть (или Иметь опыт деятельности): навыками применения применения информационной безопасности Владеть (или Иметь опыт деятельности): навыками оценки применения применения информационной безопасности ПК-11.4 Знать: базовые Формулиру безопасности безопасности Владеть (или Иметь опыт деятельности): навыками оценки праультативности применения праультативности применения п			информационной	информационной	информационной
Иметь опыт деятельности): навыками применения применения информационной безопасности безопасности ПК-11.4 Дермулиру Технологии, Иметь опыт деятельностии; деятельностии; навыками оценки применения			безопасности	безопасности	безопасности
результативности применения празличных средств применения празличных средств обеспечения информационной безопасности информационной безопасности ПК-11.4 Знать: базовые Формулиру технологии, технологии, технологии,			Владеть (или	Владеть (или	Владеть (или
навыками применения применения применения обеспечения информационной безопасности безопасности ПК-11.4 Знать: базовые Формулиру технологии, навыками оценки результативности применения применения применения различных средств информационной обеспечения информационной безопасности информационной безопасности знать: основные технологии, технологии, технологии,			Иметь опыт	Иметь опыт	Иметь опыт
применения штатных средств обеспечения информационной безопасности безопасности ПК-11.4 Знать: базовые Формулиру технологии, применения празличных средств обеспечения информационной безопасности знать: меры и технологии, технологии,			деятельности):	деятельности):	деятельности):
ПК-11.4 Знать: базовые Формулиру технологии, применения применения применения применения применения применения применения применения применения празличных средств применения празличных средств применения празличных средств обеспечения информационной обеспечения информационной безопасности Знать: меры и технологии, технологии,			навыками	навыками оценки	сформированными
штатных средств обеспечения информационной безопасности безопасности ПК-11.4 Формулиру технологии, применения применения применения различных средств информационной безопасности информационной безопасности знать: меры и технологии, технологии,			применения	результативности	навыками оценки
обеспечения информационной безопасности безопасности безопасности информационной безопасности безопасности обеспечения информационной безопасности информационной безопасности безопасности обеспечения информационной безопасности обеспечения информационной безопасности обеспечения информационной безопасности обеспечения информационной обеспечения информационно и			=		результативности
информационной безопасности информационной безопасности информационной безопасности информационной безопасности ПК-11.4 Знать: базовые Формулиру технологии, технологии, технологии, технологии,			-	-	
безопасности информационной обеспечения информационной безопасности ПК-11.4 Знать: базовые Формулиру технологии, технологии, технологии, технологии,			информационной	_	-
ПК-11.4 Знать: базовые Формулиру Знать: основные технологии, Знать: меры и технологии, Знать: технологии, знать: меры и технологии,			безопасности	информационной	обеспечения
ПК-11.4 Знать: базовые Формулиру технологии, Технологии, Технологии, Технологии, Технологии,					информационной
Формулиру технологии, технологии, технологии,					
		ПК-11.4	<i>Знать:</i> базовые	<i>Знать:</i> основные	Знать: меры и
ет направленные на направленные на направленные на		Формулиру	технологии,	технологии,	-
таправленные на паправленные на паправленные на		ет	направленные на	направленные на	направленные на
предложени повышение повышение повышение		предложени	повышение	повышение	повышение

1	2	3	4	5	
	я по	защищённости	защищённости	защищённости	
	совершенст	процессов	процессов	процессов	
	вованию	обработки	обработки	обработки	
	подсистем	информации в ТКС	информации в ТКС	информации в ТКС	
	обеспечени	Уметь: определять	Уметь: определять	<i>Уметь:</i> определять	
	Я	отдельные меры и	меры и технологии,	меры и технологии,	
	информаци	технологии,	направленные на	направленные на	
	онной	направленные на	повышение	повышение	
	безопасност	повышение	защищённости	защищённости	
	И	защищённости	процессов	процессов	
		процессов	обработки	обработки	
		обработки	информации в	информации в	
		информации в	конкретной ТКС	сложных ТКС	
		конкретной ТКС	Владеть (или	Владеть (или	
		Владеть (или	Иметь опыт	Иметь опыт	
		Иметь опыт	деятельности):	деятельности):	
		деятельности):	обеспечения	обеспечения	
		проведения	процесса защиты	процесса защиты	
		отдельных	информации в ТКС	информации в	
		процедур защиты		сложных ТКС	
		информации в ТКС			

6.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения основной профессиональной образовательной программы

Таблица 6.3 — Контрольные задания и иные материалы для оценки результатов обучения по практике (знаний, умений, навыков и (или) опыта деятельности)

Var var management /====	Two and the work of the second state of the se				
Код компетенции/этап	Типовые контрольные задания или иные материалы,				
формирования	необходимые для оценки знаний, умений, навыков				
компетенции	и (или) опыта деятельности				
в процессе освоения					
ОПОП ВО					
(указывается название					
этапа из п.б.1)					
ПК-1	Дневник практики.				
завершающий	Отчёт по практике с результатами измерений и отчётов				
ПК-6	Дневник практики.				
завершающий	Отчет о практике.				
_	Доклад обучающегося на промежуточной аттестации (защита				
	отчета о практике).				
	Характеристика руководителя практики от организации				
	управленческих качеств обучающегося.				
ПК-7	Дневник практики.				
завершающий	Отчет о практике.				

ПК-8 завершающий Отчет о практике. Типовое задание № 2 по практической подготовке, предусматривающее выполнение обучающимся вида(ов) работ, связанного(ых) с будущей профессиональной деятельностью (задание конкретизируется с учетом особенностей конкретной профильной организации в Дневнике практики, в п.1.4 задания студенту): разработать модель угроз оля объекта информатизации, на котором происходит эксплуатация телекоммуникационной ситсемы. Разработанные модели угроз Ответы на вопросы по содержанию практики на промежуточной аттестации. ПК-9 завершающий Типовое задание № 3 по практической подготовке, предусматривающее выполнение обучающимся вида(ов) работ, связанного(ых) с будущей профессиональной деятельностью (задание конкретизируется с учетом особенностей конкретной профильной организации в Дневнике практики, в п.1.4 задания студенту): Разработайте рекомендации по повышению уровня безопасности предприятия, основываясь на результатах проведенного мониторинга (производственного контроля). Графические материалы к отчету. Раздел отчета о практике — Результать проведенного мониторинга (и (или) производственного контроля) работоспособности ТКС. ПК-10 завершающий Дневник практики. Отчета о практике: — Профили защиты используемых средств обеспечения информационной безопасностии. Защищённости ТКС. Пк-11 завершающий Отчета о практике: Доклад обучающегося на промежуточной аттестации (защита отчета о практике).		Типовое задание № 1 по практической подготовке, предусматривающее выполнение обучающимся вида(ов) работ, связанного(ых) с будущей профессиональной деятельностью (задание конкретизируется с учетом особенностей конкретной профильной организации в Дневнике практики, в п.1.4 задания студенту): Подготовьте паспорт объекта информатизации для проведения аттестационных испытаний по защите информации. Ответы на вопросы по содержанию практики на промежуточной аттестации.
Типовое задание № 2 по практической подготовке, предусматривающее выполнение обучающимся вида(ов) работ, связанного(ых) с будущей профессиональной деятельностью (задание конкретизируется с учетом особенностей конкретной профильной организации в Дневнике практики, в п.1.4 задания студенту): разработать модель угроз для объекта информатизации, на котором происходит эксплуатация телекоммуникационной ситсемы. Разработанные модели угроз Ответы на вопросы по содержанию практики на промежуточной аттестации. ПК-9 Дневник практики. Типовое задание № 3 по практической подготовке, предусматривающее выполнение обучающимся вида(ов) работ, связанного(ых) с будущей профессиональной деятельностью (задание конкретизируется с учетом особенностей конкретной профильной организации в Дневнике практики, в п.1.4 задания студенту): Разработайте рекомендации по повышению уровня безопасности предприятия, основываясь на результатах проведенного мониторинга (производственного контроля). Графические материалы к отчету. Раздел отчета о практике — Результаты проведенного мониторинга (и (или) производственного контроля) работоспособности ТКС. ПК-10 Дневник практики. Завершающий Разделы отчета о практике: — Профили защиты используемых средств обеспечения информационной безопасностии. Защищённости ТКС. ПК-11 Завершающий Отчета о практике: Доклад обучающегося на промежуточной аттестации (защита отчета о практике).	ПК-8	
предусматривающее выполнение обучающимся вида(ов) работ, связанного(ых) с будущей профессиональной деятельностью (задание конкретизируется с учетом особенностей конкретной профильной организации в Дневнике практики, в п.1.4 задания студенту): разработать модель угроз для объекта информатизации, на котором происходит эксплуатация телекоммуникационной ситсемы. Разработанные модели угроз Ответы на вопросы по содержанию практики на промежуточной аттестации. ПК-9 Дневник практики. Завершающий Типовое задание № 3 по практической подготовке, предусматривающее выполнение обучающимся вида(ов) работ, связанного(ых) с будущей профессиональной деятельностью (задание конкретизируется с учетом особенностей конкретной профильной организации в Дневнике практики, в п.1.4 задания студенту): Разработайте рекомендации по повышению уровня безопасностии предприятия, основываясь на результатах проведенного мониторинга (производственного контроля). Графические материалы к отчету. Раздел отчета о практике — Результаты проведенного мониторинга (и (или) производственного контроля) работоспособности ТКС. ПК-10 Дневник практики. Разделы отчета о практике: — Профили защиты используемых средств обеспечения информационной безопасностии. — Защищённости ТКС. ПК-11 Завершающий Отчета о практике: Доклад обучающегося на промежуточной аттестации (защита отчета о практике).		
связанного(ых) с будущей профессиональной деятельностью (задание конкретизируется с учетом особенностей конкретной профильной организации в Дневнике практики, в п.1.4 задания студенту): разработать модель угроз для объекта информатизации, на котором происходит эксплуатация телекоммуникационной ситсемы. Разработанные модели угроз Ответы на вопросы по содержанию практики на промежуточной аттестации. ПК-9 Дневник практики. Типовое задание № 3 по практической подготовке, предусматривающее выполнение обучающимся вида(ов) работ, связанного(ых) с будущей профессиональной деятельностью (задание конкретизируется с учетом особенностей конкретной профильной организации в Дневнике практики, в п.1.4 задания студенту): Разработайте рекомендации по повышению уровня безопасности предприятия, основываясь на результатах проведенного мониторинга (производственного контроля). Графические материалы к отчету. Раздел отчета о практике — Результаты проведенного мониторинга (и (или) производственного контроля) работоспособности ТКС. ПК-10 Дневник практики. Разделы отчета о практике: — Профили защиты используемых средств обеспечения информационной безопасностии. — Защищённости ТКС. ПК-11 Завершающий Отчета о практике: Доклад обучающегося на промежуточной аттестации (защита отчета о практике).	завершатещий	
(задание конкретизируется с учетом особенностей конкретной профильной организации в Дневнике практики, в п.1.4 задания студенту): разработать модель угроз для объекта информатизации, на котором происходит эксплуатация телекоммуникационной ситсемы. Разработанные модели угроз Ответы на вопросы по содержанию практики на промежуточной аттестации. ПК-9 Завершающий Типовое задание № 3 по практической подготовке, предусматривающее выполнение обучающимся вида(ов) работ, связанного(ых) с будущей профессиональной деятельностью (задание конкретизируется с учетом особенностей конкретной профильной организации в Дневнике практики, в п.1.4 задания студенту): Разработвайше рекомендации по повышению уровня безопасности предприятия, основываясь на результатах проведенного мониторинга (производственного контроля). Графические материалы к отчету. Раздел отчета о практике — Результаты проведенного мониторинга (и (или) производственного контроля) работноспособности ТКС. ПК-10 Завершающий Разделы отчета о практике: — Профили защиты используемых средств обеспечения информационной безопасности. — Защищённости ТКС. ПК-11 Завершающий Отчета о практике: Доклад обучающегося на промежуточной аттестации (защита отчета о практике).		
профильной организации в Дневнике практики, в п.1.4 задания студенту): разработать модель угроз для объекта информатизации, на котором происходит эксплуатация телекоммуникационной ситсемы. Разработанные модели угроз Ответы на вопросы по содержанию практики на промежуточной аттестации. ПК-9 Завершающий Дневник практики. Типовое задание № 3 по практической подготовке, предусматривающее выполнение обучающимся вида(ов) работ, связанного(ых) с будущей профессиональной деятельностью (задание конкретизируется с учетом особенностей конкретной профильной организации в Дневнике практики, в п.1.4 задания студенту): Разработайте рекомендации по повышению уровня безопасности предприятия, основываясь на результатах проведенного мониторинга (производственного контроля). Графические материалы к отчету. Раздел отчета о практике — Результаты проведенного мониторинга (и (или) производственного контроля) работоспособности ТКС. ПК-10 Завершающий Разделы отчета о практике: — Профили защиты используемых средств обеспечения информационной безопасности. — Защицённости ТКС. ПК-11 Завершающий Отчета о практике: Доклад обучающегося на промежуточной аттестации (защита отчета о практике).		
студенту): разработать модель угроз для объекта информатизации, на котором происходит эксплуатация телекоммуникационной ситсемы. Разработанные модели угроз Ответы на вопросы по содержанию практики на промежуточной аттестации. ПК-9 Завершающий Типовое задание № 3 по практической подготовке, предусматривающее выполнение обучающимся вида(ов) работ, связанного(ых) с будущей профессиональной деятельностью (задание конкретизируется с учетом особенностей конкретной профильной организации в Дневнике практики, в п.1.4 задания студенту): Разработайте рекомендации по повышению уровня безопасности предприятия, основываясь на результатах проведенного мониторинга (производственного контроля). Графические материалы к отчету. Раздел отчета о практике — Результаты проведенного мониторинга (и (или) производственного контроля) работослособности ТКС. ПК-10 Дневник практики. Завершающий Разделы отчета о практике: — Профили защиты используемых средств обеспечения информационной безопасности. — Защищённости ТКС. ПК-11 Завершающий Отчета о практики: Доклад обучающегося на промежуточной аттестации (защита отчета о практике).		
разработанные модели угроз Ответы на вопросы по содержанию практики на промежуточной аттестации. ПК-9 Дневник практики. Типовое задание № 3 по практической подготовке, предусматривающее выполнение обучающимся вида(ов) работ, связанного(ых) с будущей профессиональной деятельностью (задание конкретизируется с учетом особенностей конкретной профильной организации в Дневнике практики, в п.1.4 задания студенту): Разработайте рекомендации по повышению уровня безопасности преоприятия, основываясь на результатах проведенного мониторинга (производственного контроля). Графические материалы к отчету. Раздел отчета о практике — Результаты проведенного мониторинга (и (или) производственного контроля) работоспособности ТКС. ПК-10 Дневник практики. Разделы отчета о практике: — Профили защиты используемых средств обеспечения информационной безопасности. — Защищённости ТКС. ПК-11 Завершающий Отчета о практике: Доклад обучающегося на промежуточной аттестации (защита отчета о практике).		
разработанные модели угроз Ответы на вопросы по содержанию практики на промежуточной аттестации. ПК-9 Дневник практики. Типовое задание № 3 по практической подготовке, предусматривающее выполнение обучающимся вида(ов) работ, связанного(ых) с будущей профессиональной деятельностью (задание конкретизируется с учетом особенностей конкретной профильной организации в Дневнике практики, в п.1.4 задания студенту): Разработайте рекомендации по повышению уровня безопасности преоприятия, основываясь на результатах проведенного мониторинга (производственного контроля). Графические материалы к отчету. Раздел отчета о практике — Результаты проведенного мониторинга (и (или) производственного контроля) работоспособности ТКС. ПК-10 Дневник практики. Разделы отчета о практике: — Профили защиты используемых средств обеспечения информационной безопасности. — Защищённости ТКС. ПК-11 Завершающий Отчета о практике: Доклад обучающегося на промежуточной аттестации (защита отчета о практике).		информатизации, на котором происходит эксплуатация
Ответы на вопросы по содержанию практики на промежуточной аттестации. ПК-9 Дневник практики. Типовое задание № 3 по практической подготовке, предусматривающее выполнение обучающимся вида(ов) работ, связанного(ых) с будущей профессиональной деятельностью (задание конкретизируется с учетом особенностей конкретной профильной организации в Дневнике практики, в п.1.4 задания студенту): Разработайте рекомендации по повышению уровня безопасностии предоприятия, основываясь на результатах проведенного мониторинга (производственного контроля). Графические материалы к отчету. Раздел отчета о практике — Результаты проведенного мониторинга (и (или) производственного контроля) работоспособности ТКС. ПК-10 Дневник практики. Разделы отчета о практике: — Профили защиты используемых средств обеспечения информационной безопасностии. — Защищённости ТКС. ПК-11 Завершающий Отчета о практике: Доклад обучающегося на промежуточной аттестации (защита отчета о практике).		телекоммуникационной ситсемы.
ПК-9 Завершающий Типовое задание № 3 по практической подготовке, предусматривающее выполнение обучающимся вида(ов) работ, связанного(ых) с будущей профессиональной деятельностью (задание конкретизируется с учетом особенностей конкретной профильной организации в Дневнике практики, в п.1.4 задания студенту): Разработайте рекомендации по повышению уровня безопасности предприятия, основываясь на результатах проведенного мониторинга (производственного контроля). Графические материалы к отчету. Раздел отчета о практике — Результаты проведенного мониторинга (и (или) производственного контроля) работоспособности ТКС. ПК-10 Дневник практики. Разделы отчета о практике: — Профили защиты используемых средств обеспечения информационной безопасности. — Защищённости ТКС. ПК-11 Завершающий Отчета о практике: Доклад обучающегося на промежуточной аттестации (защита отчета о практике).		
 ПК-9 Завершающий Типовое задание № 3 по практической подготовке, предусматривающее выполнение обучающимся вида(ов) работ, связанного(ых) с будущей профессиональной деятельностью (задание конкретизируется с учетом особенностей конкретной профильной организации в Дневнике практики, в п.1.4 задания студенту): Разработайте рекомендации по повышению уровня безопасности предприятия, основываясь на результатах проведенного мониторинга (производственного контроля). Графические материалы к отчету. Раздел отчета о практике — Результаты проведенного мониторинга (и (или) производственного контроля) работоспособности ТКС. ПК-10 Дневник практики. Разделы отчета о практике: Профили защиты используемых средств обеспечения информационной безопасности. Защищённости ТКС. ПК-11 Дневник практики. Завершающий Отчета о практике: 		
типовое задание № 3 по практической подготовке, предусматривающее выполнение обучающимся вида(ов) работ, связанного(ых) с будущей профессиональной деятельностью (задание конкретизируется с учетом особенностей конкретной профильной организации в Дневнике практики, в п.1.4 задания студенту): Разработайте рекомендации по повышению уровня безопасности предприятия, основываясь на результатах проведенного мониторинга (производственного контроля). Графические материалы к отчету. Раздел отчета о практике — Результаты проведенного мониторинга (и (или) производственного контроля) работоспособности ТКС. ПК-10 Дневник практики. завершающий Разделы отчета о практике: — Профили защиты используемых средств обеспечения информационной безопасности. — Защищённости ТКС. ПК-11 Дневник практики. Отчета о практике: Доклад обучающегося на промежуточной аттестации (защита отчета о практике).		
предусматривающее выполнение обучающимся вида(ов) работ, связанного(ых) с будущей профессиональной деятельностью (задание конкретизируется с учетом особенностей конкретной профильной организации в Дневнике практики, в п.1.4 задания студенту): Разработайте рекомендации по повышению уровня безопасности предприятия, основываясь на результатах проведенного мониторинга (производственного контроля). Графические материалы к отчету. Раздел отчета о практике — Результаты проведенного мониторинга (и (или) производственного контроля) работоспособности ТКС. ПК-10 Дневник практики. Разделы отчета о практике: — Профили защиты используемых средств обеспечения информационной безопасности. — Защищённости ТКС. ПК-11 Завершающий Отчета о практики. Отчета о практики. Отчета о практике: Доклад обучающегося на промежуточной аттестации (защита отчета о практике).		
Разделы отчета о практике: — Профили защиты используемых средств обеспечения информационной безопасности. — Защищённости ТКС. ПК-11 Завершающий Отчета о практики. Доклад обучающегося на промежуточной аттестации (защита отчета о практике).		предусматривающее выполнение обучающимся вида(ов) работ, связанного(ых) с будущей профессиональной деятельностью (задание конкретизируется с учетом особенностей конкретной профильной организации в Дневнике практики, в п.1.4 задания студенту): Разработайте рекомендации по повышению уровня безопасности предприятия, основываясь на результатах проведенного мониторинга (производственного контроля). Графические материалы к отчету. Раздел отчета о практике — Результаты проведенного мониторинга (и (или) производственного контроля) работоспособности ТКС.
 Профили защиты используемых средств обеспечения информационной безопасности. Защищённости ТКС. ПК-11 Дневник практики. Отчета о практике: Доклад обучающегося на промежуточной аттестации (защита отчета о практике). 		
информационной безопасности. — Защищённости ТКС. ПК-11 Завершающий Отчета о практике: Доклад обучающегося на промежуточной аттестации (защита отчета о практике).	завершающии	
— Защищённости ТКС. ПК-11 Дневник практики. завершающий Отчета о практике: Доклад обучающегося на промежуточной аттестации (защита отчета о практике).		
ПК-11 Дневник практики. завершающий Отчета о практике: Доклад обучающегося на промежуточной аттестации (защита отчета о практике).		
Завершающий Отчета о практике: Доклад обучающегося на промежуточной аттестации (защита отчета о практике).	ПК-11	
Доклад обучающегося на промежуточной аттестации (защита отчета о практике).		1 ' '
отчета о практике).	эшэсршиющий	
Характеристика руководителя практики от организации		77
управленческих качеств обучающегося.		

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

Оценка знаний, умений, навыков, характеризующая этапы формирования компетенций, закрепленных за производственной преддипломной практикой, осуществляется в форме текущего контроля успеваемости и промежуточной аттестации обучающихся.

Текущий контроль успеваемости проводится в течение практики на месте ее проведения руководителем практики от организации.

Промежуточная аттестация обучающихся проводится в форме зачета с оценкой. На зачет обучающийся представляет дневник практики и отчет о практике. Зачет проводится в виде устной защиты отчета о практике.

Таблица 6.4.1 – Шкала оценки отчета о практике и его защиты

№	Предмет оценки	Критерии оценки	Максимальный балл
1	Содержание отчета	Достижение цели и выполнение	1
	10 баллов	задач практики в полном объеме	
		Отражение в отчете всех	1
		предусмотренных программой	
		практики видов работ, связанных с	
		будущей профессиональной	
		деятельностью	
		Владение актуальными	1
		нормативными правовыми	
		документами и профессиональной	
		терминологией	
		Соответствие структуры и	1
		содержания отчета требованиям,	
		установленным в п. 5 настоящей	
		программы	
		Полнота и глубина раскрытия	1
		содержания разделов отчета	
		Достоверность и достаточность	1
		приведенных в отчете данных	
		Правильность выполнения	1
		расчетов и измерений	
		Глубина анализа данных	1
		Обоснованность выводов и	1
		рекомендаций	
		Самостоятельность при	1
		подготовке отчета	
2	Оформление отчета	Соответствие оформления отчета	1
	2 балла	требованиям, установленным в п.5	
		настоящей программы	
		Достаточность использованных	1
		источников	
3	Содержание и оформление	Полнота и соответствие	2
	презентации (графического материала)	содержания презентации	
	4 балла	(графического материала)	
		содержанию отчета	

		Грамотность речи и правильность использования профессиональной	2
		терминологии	4
4	Ответы на вопросы о содержании	Полнота, точность,	4
	практики, в том числе на вопросы о	аргументированность ответов,	
	практической подготовке (видах		
	работ, связанных с будущей		
	профессиональной деятельностью,		
	выполненных на практике)		
	4 балла		

Примечание 1 — Записи в строках 1 и 4 о видах работ, связанных с будущей профессиональной деятельностью, вносятся в данный раздел в рабочих программах всех учебных и производственных практик, указанных в учебном плане.

Баллы, полученные обучающимся, суммируются, соотносятся с уровнем сформированности компетенций и затем переводятся в оценки по 5-балльной шкале.

Таблица 6.4.2 — Соответствие баллов уровням сформированности компетенций и оценкам по 5-балльной шкале

Баллы	Уровень сформированности компетенций	Оценка по 5-балльной шкале (зачет с оценкой)
18-20	высокий	отлично
14-17	продвинутый	хорошо
10-13	пороговый	удовлетворительно
9 и менее	недостаточный	неудовлетворительно

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

Основная литература:

- 1. Информационная безопасность и защита информации [Текст] : учебное пособие / Ю. Ю. Громов [и др.]. Старый Оскол : ТНТ, 2013. 384 с.
- 2. Нестеров, С. А. Основы информационной безопасности: учебное пособие / С. А. Нестеров; Санкт-Петербургский государственный политехнический университет. СПб.: Издательство Политехнического университета, 2014. 322 с. URL: http://biblioclub.ru/index.php?page=book&id=363040 (дата обращения

http://biblioclub.ru/index.php?page=book&id=363040 (дата обращения 02.09.2021) . - Режим доступа: по подписке. - Текст : электронный.

3. Степанова, Е. Е. Информационное обеспечение управленческой деятельности [Текст] : учебное пособие / Е. Е. Степанова, Н. В. Хмелевская. - М. : Фо-рум, 2004. - 154 с.

Дополнительная литература:

- Аверченков, В. И. Аудит информационной безопасности [Электронный ресурс]: учебное пособие для вузов / В. И. Аверченков. - 3-е стереотип. M. Флинта, 2016. 269 URL: http://biblioclub.ru/index.php?page=book&id=93245 (дата обращения 02.09.2021) . - Режим доступа: по подписке. - Текст : электронный.
- 5) Абрамов, Г. В. Проектирование информационных систем: учебное пособие / Г. В. Абрамов, И. Медведкова, Л. Коробова. Воронеж: Воронежский государственный университет инженерных технологий, 2012. 172 с. URL: http://biblioclub.ru/index.php?page=book&id=141626 (дата обращения 03.09.2021). Режим доступа: по подписке. ISBN 978-5-89448-953-7. Текст: электронный.
- 6) Древс, Ю. Г. Организация ЭВМ и вычислительных систем [Текст] : учебник / Ю. Г. Древс. М. : Высшая школа, 2006. 501 с.
- 7) Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации: учебное пособие / Ю. Н. Загинайлов. М.; Берлин: Директ-Медиа, 2015. 253 с. URL: http://biblioclub.ru/index.php?page=book&id=276557 (дата обращения 31.08.2021). Режим доступа: по подписке. Текст: электронный.
- 8) Куль, Т. П. Операционные системы: учебное пособие / Т. П. Куль. Минск: РИПО, 2015. 312 с. URL: http://biblioclub.ru/index.php?page=book&id=463629 (дата обращения 02.09.2021). Режим доступа: по подписке. Текст: электронный.
- 9) Лопин, В. Н. Защита информации в компьютерных системах [Текст] : учебное пособие / В. Н. Лопин, И. С. Захаров, А. В. Николаев ; Министерство образования и науки Российской Федерации, Курский государственный технический университет. Курск : КГТУ, 2006. 159 с.
- 10) Олифер, В. Г. Сетевые операционные системы [Текст]: учебное пособие / В. Г. Олифер, Н. А. Олифер. СПб.: Питер, 2003. 539 с.
- 11) Петренко, В .И. Теоретические основы защиты информации : учебное пособие / В. И. Петренко ; Северо-Кавказский федеральный университет. Ставрополь : СКФУ, 2015. 222 с. URL: http://biblioclub.ru/index.php?page=book&id=458204 (дата обращения 02.09.2021) . Режим доступа: по подписке. Текст : электронный.
- 12) ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»
- 13) ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»
- 14) Р 50.1.056-2005 «Техническая защита информации. Основные термины и определения»
- 15) ГОСТ Р ИСО/МЭК 15408-1-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель»

- 16) ГОСТ Р ИСО/МЭК 15408-2-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности»
- 17) ГОСТ Р ИСО/МЭК 15408-3-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности»
- 18) ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью»
- 19) ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»
- 20) ГОСТ Р ИСО/МЭК 13335-1-2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий»
- 21) ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий»
- 22) ГОСТ Р ИСО/МЭК ТО 13335-4-2007 «Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер»
- 23) ГОСТ Р ИСО/МЭК ТО 13335-5-2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети»
- 24) ГОСТ Р ИСО/ТО 13569-2007 «Финансовые услуги. Рекомендации по информационной безопасности»
- 25) ГОСТ Р ИСО/МЭК 15026-2002 «Информационная технология. Уровни целостности систем и программных средств»
- 26) ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности»
- 27) ГОСТ Р ИСО/МЭК 18045-2008 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий»
- 28) ГОСТ Р ИСО/МЭК 19794-2-2005 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 2. Данные изображения отпечатка пальца контрольные точки»
- 29) ГОСТ Р ИСО/МЭК 19794-4-2006 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 4. Данные изображения отпечатка пальца»

- 30) ГОСТ Р ИСО/МЭК 19794-5-2006 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица»
- 31) ГОСТ Р ИСО/МЭК 19794-6-2006 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 6. Данные изображения радужной оболочки глаза»
- 32) ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования»
- 33) ГОСТ Р 51188-98 «Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство»
- 34) ГОСТ Р 51725.6-2002 «Каталогизация продукции для федеральных государственных нужд. Сети телекоммуникационные и базы данных. Требования информационной безопасности»
- 35) ГОСТ Р 51898-2002 «Аспекты безопасности. Правила включения в стандарты»
- 36) ГОСТ Р 52069.0-2003 «Защита информации. Система стандартов. Основные положения»
- 37) ГОСТ Р 52447-2005 «Защита информации. Техника защиты информации. Номенклатура показателей качества»
- 38) ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»
- 39) ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»
- 40) ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хеширования»
- 41) Стандарт Банка России: «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (СТО БР ИББС-1.0-2008)
- 42) Стандарт Банка России: «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности» (СТО БР ИББС-1.1-2007)
- 43) Стандарт Банка России: «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям стандарта СТО БР ИББС-1.0-2008» (СТО БР ИББС-1.2-2009)
- 44) Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС-1.0» (РС БР ИББС-2.0-2007)

- 45) Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Руководство по самооценке соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям стандарта СТО БР ИББС-1.0» (РС БР ИББС-2.1-2007)
- 46) Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности» (РС БР ИББС-2.2-2009)
- 47) Описание формы предоставления результатов оценки уровня информационной безопасности организаций банковской системы Российской Федерации

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

- 1. Федеральная служба безопасности [официальный сайт]. Режим доступа: http://www.fsb.ru/
- 2. Федеральная служба по техническому и экспортному контролю [официальный сайт]. Режим доступа: http://fstec.ru/
- 3. Сообщество Ubuntu [официальный сайт]. Режим доступа: http://ubuntu.com/
- 4. Корпорация Microsoft [официальный сайт]. Режим доступа: http://microsoft.com/
- 5. <u>Компания «Консультант Плюс» [официальный сайт]</u>. Режим доступа: http://www.consultant.ru

8 Перечень информационных технологий, используемых при проведении практики, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

- 1. Научно-информационный портал ВИНИТИ РАН [официальный сайт]. Режим доступа: http://www.consultant.ru/
 - 2. База данных "Патенты России"
- 3. Электронно-библиотечная система «Университетская библиотека онлайн» Режим доступа: http://biblioclub.ru
- 4. Электронная библиотека диссертаций и авторефератов РГБ http://dvs.rsl.ru

9 Описание материально-технической базы, необходимой для проведения практики

Для проведения практики используется оборудование конкретной профильной организации, на базе которой она проводится: современная измерительная техника: устройства, позволяющие осуществлять контроль

защищённости, программные и аппаратные системы защиты информации, обрабатываемых в телекоммуникационных системах, и устройства, позволяющие фиксировать параметры микроклимата (межсетевые экраны, роутеры, маршрутизаторы, коммутаторы, системы виброакустического зашумления, датчики, акустические излучатели, подавители «жучков» и беспроводных видеокамер, поисковые приборы, генераторы шума);

Для осуществления практической подготовки обучающихся при реализации практики используются оборудование и технические средства обучения конкретной(-ых) профильной(-ых) организации(-й), в которых она проводится:

межсетевые экраны, роутеры, маршрутизаторы, коммутаторы, системы виброакустического зашумления, датчики , акустические излучатели, подавители «жучков» и беспроводных видеокамер , поисковые приборы, генераторы шума

Для проведения промежуточной аттестации обучающихся по практике используется следующее материально-техническое оборудование:

- 1. Класс ПЭВМ Asus-P7P55LX-/DDR34096Mb/Coree i3-540/SATA-11 500 Gb Hitachi/PCI-E 512Mb, Монитор TFT Wide 23.
- 2. Мультимедиацентр: ноутбук ASUS X50VL PMD T2330/14"/1024Mb/ 160Gb/ сумка/проектор inFocus IN24+ .
 - 3. Экран мобильный Draper Diplomat 60x60

10 Особенности организации и проведения практики для инвалидов и лиц с ограниченными возможностями здоровья

Практика для обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (далее – OB3) организуется и проводится на основе индивидуального личностно ориентированного подхода.

Обучающиеся из числа инвалидов и лиц с ОВЗ могут проходить практику как совместно с другими обучающимися (в учебной группе), так и индивидуально (по личному заявлению).

Определение места практики

Выбор мест прохождения практики для инвалидов и лиц с ОВЗ осуществляется с учетом требований их доступности для данной категории обучающихся. При определении места прохождения практики для инвалидов и лиц с ОВЗ учитываются рекомендации медико-социальной экспертизы, отраженные в индивидуальной программе реабилитации инвалида (при наличии), относительно рекомендованных условий и видов труда. При необходимости для прохождения практики создаются специальные рабочие места в соответствии с характером нарушений, а также с учетом выполняемых обучающимся-инвалидом или обучающимся с ОВЗ трудовых функций, вида профессиональной деятельности и характера труда.

Обучающиеся данной категории могут проходить практику в профильных организациях, определенных для учебной группы, в которой они обучаются, если это не создает им трудностей в прохождении практики и освоении программы практики.

При наличии необходимых условий для освоения программы практики и выполнения индивидуального задания (или возможности создания таких условий) практика обучающихся данной категории может проводиться в структурных подразделениях ЮЗГУ.

При определении места практики для обучающихся из числа инвалидов и лиц с ОВЗ особое внимание уделяется безопасности труда и оснащению (оборудованию) рабочего места. Рабочие места, предоставляемые профильной организацией, должны (по возможности) соответствовать следующим требованиям:

- для инвалидов по зрению-слабовидящих: оснащение специального рабочего места общим и местным освещением, обеспечивающим беспрепятственное нахождение указанным лицом своего рабочего места и выполнение трудовых функций, видеоувеличителями, лупами;
- для инвалидов по зрению-слепых: оснащение специального рабочего места тифлотехническими ориентирами и устройствами, с возможностью использования крупного рельефно-контрастного шрифта и шрифта Брайля, акустическими навигационными средствами, обеспечивающими беспрепятственное нахождение указанным лицом своего рабочего места и выполнение трудовых функций;
- для инвалидов по слуху-слабослышащих: оснащение (оборудование) специального рабочего места звукоусиливающей аппаратурой, телефонами громкоговорящими;
- для инвалидов по слуху-глухих: оснащение специального рабочего места визуальными индикаторами, преобразующими звуковые сигналы в световые, речевые сигналы в текстовую бегущую строку, для беспрепятственного нахождения указанным лицом своего рабочего места и выполнения работы;
- для инвалидов с нарушением функций опорно-двигательного аппарата: оборудование, обеспечивающее реализацию эргономических принципов (максимально удобное для инвалида расположение элементов, составляющих рабочее место), механизмами и устройствами, позволяющими изменять высоту и наклон рабочей поверхности, положение сиденья рабочего стула по высоте и наклону, угол наклона спинки рабочего стула, оснащение специальным сиденьем, обеспечивающим компенсацию усилия при вставании, специальными приспособлениями для управления и обслуживания этого оборудования.

Особенности содержания практики

Индивидуальные задания формируются руководителем практики от университета с учетом особенностей психофизического развития,

индивидуальных возможностей и состояния здоровья каждого конкретного обучающегося данной категории и должны соответствовать требованиям выполнимости и посильности.

При необходимости (по личному заявлению) содержание практики может быть полностью индивидуализировано (при условии сохранения возможности формирования у обучающегося всех компетенций, закрепленных за данной практикой).

Особенности организации трудовой деятельности обучающихся

Объем, темп, формы работы устанавливаются индивидуально для каждого обучающегося данной категории. В зависимости от нозологии максимально снижаются противопоказанные (зрительные, звуковые, мышечные и др.) нагрузки.

Применяются методы, учитывающие динамику и уровень работоспособности обучающихся из числа инвалидов и лиц с ОВЗ. Для предупреждения утомляемости обучающихся данной категории после каждого часа работы делаются 10-15-минутные перерывы.

Для формирования умений, навыков и компетенций, предусмотренных программой практики, производится большое количество повторений (тренировок) подлежащих освоению трудовых действий и трудовых функций.

Особенности руководства практикой

Осуществляется комплексное сопровождение инвалидов и лиц с OB3 во время прохождения практики, которое включает в себя:

- учебно-методическую и психолого-педагогическую помощь и контроль со стороны руководителей практики от университета и от организации;
- корректирование (при необходимости) индивидуального задания и программы практики;
- помощь ассистента (ассистентов) и (или) волонтеров из числа обучающихся работников профильной организации. ИЛИ Ассистенты/волонтеры оказывают обучающимся данной категории необходимую техническую помощь при входе в здания и помещения, в которых проводится практика, и выходе из них; размещении на рабочем месте; передвижении по помещению, в котором проводится практика; ознакомлении с индивидуальным заданием и его выполнении; оформлении дневника и составлении отчета о практике; общении с руководителями практики.

Особенности учебно-методического обеспечения практики

Учебные и учебно-методические материалы по практике представляются в различных формах так, чтобы инвалиды с нарушениями слуха получали информацию визуально (программа практики и индивидуальное задание на практику печатаются увеличенным шрифтом;

предоставляются видеоматериалы и наглядные материалы по содержанию практики), с нарушениями зрения — аудиально (например, с использованием программ-синтезаторов речи) или с помощью тифлоинформационных устройств.

Особенности проведения текущего контроля успеваемости и промежуточной аттестации

Во время проведения текущего контроля успеваемости и промежуточной аттестации разрешаются присутствие и помощь ассистентов (сурдопереводчиков, тифлосурдопереводчиков и др.) и (или) волонтеров и оказание ими помощи инвалидам и лицам с ОВЗ.

Форма проведения текущего контроля успеваемости и промежуточной аттестации для обучающихся-инвалидов и лиц с ОВЗ устанавливается с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.). При необходимости обучающемуся предоставляется дополнительное время для подготовки ответа и (или) защиты отчета.

11 Лист дополнений и изменений, внесенных в программу практики

	Номера страниц					Основание	
Номер изменени я	изме- ненны х	замененны х	аннулированн ых	новы Х	Всего страни ц	Дат а	для изменения и подпись лица, проводившег
							о изменения