Документ подписан простой электр	онной подписью
	фундаментальной и прикладной информатики 1:42
Уникальный программный ключ: 65ab2aa0d384efe8480e6a4c688edd	Юго-Западный государственный университет dbc475e411a
	УТВЕРЖДАЮ:
	И.о. декана факультета ФиПИ
	Таныгин М.О. (подпись, улициалы, фамилия) «
	РАБОЧАЯ ПРОГРАММА ПРАКТИКИ
	Производственная технологическая практика (наименование вида и типа практики)
ОПОП ВО	10.04.01 Информационная безопасность шифр и наименование направление подготовки (специальности)
	«Защищенные информационные системы»
	наименование направленности (профиля, специализации)
форма обуче	
	очная, очно-заочная, заочная

Курск – 2022

Рабочая программа практики составлена в соответствии с:

- федеральным государственным образовательным стандартом высшего образования – магистратура по направлению 10.04.01 Информационная безопасность, утвержденного приказом Министерства образования и науки Российской Федерации от 26 ноября 2020 г. №1455;
- учебным планом ОПОП ВО 10.04.01 Информационная безопасность, профиль «Защищенные информационные системы», 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 10.04.01 Информационная безопасность, профиль «Защищенные информационные системы» на заседании кафедры информационной безопасности «30» августа 2021 г., протокол № 6.

Зав. кафедройТаныгин М.О.
Разработчик программы
к.т.н., доцент Таныгин М.О.
(ученая степень и ученое звание, Ф.И.О.)
Marian a Mayananayag P.F.
Директор научной библиотеки Макаровская В.Г
Рабочая программа практики пересмотрена, обсуждена и рекомендова
на к реализации в образовательном процессе на основании учебного план
ОПОП ВО 10.04.01 Информационная безопасность, профиль «Защищеннь
информационные системы», одобренного Ученым советом университета про
токол № <u>7 «28</u> » <u>г., на заседании кафедры ///</u>
nportored with or 30.08.02 As
(наименование кафедры, дата, номер протокола)
Зав. кафедрой
Рабочая программа практики пересмотрена, обсуждена и рекомендова
на к реализации в образовательном процессе на основании учебного план
ОПОП ВО 10.04.01 Информационная безопасность, профиль «Защищенны
информационные системы», одобренного Ученым советом университета про
токол № 7 « 28» _ 0 2 _ 20 22 г., на заседании кафедры_ <i>U5</i>
протокой бе от 30.08.2023.
(наименование кафедры, бата, номер протокожа)
Зав. кафедрой
Рабочая программа практики пересмотрена, обсуждена и рекомендова
на к реализации в образовательном процессе на основании учебного план
ОПОП ВО 10.04.01 Информационная безопасность, профиль «Защищенны
информационные системы», одобренного Ученым советом университета про
токол № <u>«</u> » 20 г., на заседании кафедры
(наименование кафедры, дата, номер протокола)
Зав. кафедрой

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

1.1. Цель практики

Целью производственной технологической практики является получение профессиональных умений профессиональной опыта И области проектирования деятельности В реализации И технологий информационной безопасности.

1.2. Задачи практики

- 1. Формирование профессиональных компетенций, установленных ФГОС ВО и закрепленных учебным планом за производственной проектнотехнологической практикой.
- 2. Освоение современных технологий и технических средств, 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 – технологическая.

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.

Форма 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

Падили	a nanna mama a aaaaana	Код	Планируализа
Планируемые результаты освоения			Планируемые
основной профессиональной		и наименование	результаты обучения
образовательной программы		индикатора	по практике,
,	енции, закрепленные	достижения	соотнесенные с
	а практикой)	компетенции,	индикаторами
код	наименование	закрепленного	достижения компетенций
компетенции	компетенции	за практикой	
ОПК-1	Способен обосновывать	ОПК-1.1;	Знать:
	требования к системе	Проектирует	- основные угрозы
	обеспечения	информационные	информационной
	информационной	системы с учетом	безопасности;
	безопасности и	различных технологий	- возможные каналы
	разрабатывать проект	обеспечения	утечки конфиденциальной
	технического задания	информационной	информации;
	на ее создание	безопасности	- нормативно-правовые
			аспекты обеспечения
			информационной
			безопасности РФ;
			Уметь:
			- выявлять угрозы
			информационной
			безопасности;
			- снижать вероятность
			отрицательных
			последствий сетевого
			взаимодействия;
			- классифицировать угрозы
			информационной
			безопасности;
			- Владеть (или Иметь
			опыт деятельности):
			- навыками
			классификации угроз;
			- навыками выявления
			уязвимостей технических
			каналов связи
I	I	L	TIME OF THE PROPERTY OF THE PR

	74	-
е результаты освоения профессиональной программы нции, закрепленные практикой) наименование	Код и наименование индикатора достижения компетенции, закрепленного	Планируемые результаты обучения по практике, соотнесенные с индикаторами достижения компетенций
компетенции	за практикой	информационных систем.
	ОПК-1.2; Разрабатывает системы обеспечения информационной безопасности объекта	Знать: критерии оценки показателей моделируемых систем, знать методы достижения целевых показателей систем Уметь: сопоставлять результаты моделирования с изменением параметров моделирования Владеть (или Иметь опыт деятельности): навыками оптимизации параметров моделируемых
	ОПК-1.3; Планирует и оценивает трудоёмкость проекта, включая техническое, кадровое и финансовое обеспечение, принятие совместных решений	знать методологию установления зависимостей между параметрами систем и показателями их функционирования. Уметь: изменять целевые характеристики функционирования телекоммуникационных систем за счёт изменения параметров их работы Владеть (или Иметь опыт деятельности): научного обоснования решений, направленных улучшение существующих методов защиты информации
	ОПК-1.4; Формирует актуальную модель угроз для автоматизированных информационных систем и учитывает её положения при	Знать: Правовые нормы и стандарты по защите конфиденциальной информации при эксплуатации телекоммуникационной системы.
	профессиональной профессиональной программы нции, закрепленные практикой) наименование	профессиональной пельной программы ници, закрепленные компетенции закрепленного за практикой ОПК-1.2; Разрабатывает системы обеспечения информационной безопасности объекта ОПК-1.3; Планирует и оценивает трудоёмкость проекта, включая техническое, кадровое и финансовое обеспечение, принятие совместных решений ОПК-1.4; Формирует актуальную модель угроз для автоматизированных информационных систем и учитывает её

		T	
Планируемые 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 компетенций
компетенции	компетенции	за практикой	
		требований	существующий
		технического задания	инструментарий
		на проектируемую	программных и
		систему обеспечения	аппаратных средств при
		информационной	эксплуатации
		безопасности	телекоммуникационной
			системы, в том числе в
			защищённом исполнении
			Владеть (или Иметь
			опыт деятельности):
			навыками работы с
			программными и
			аппаратными средствами
			телекоммуникационной
			системы
			_
		ОПК-1.5;	<i>Знать:</i> комплекс
		Разрабатывает	мероприятий, технических
		концептуальные	мер и методов,
		стратегии решения	направленных на
		задач моделирования и	повышение защищенности
		проектирования	и снижения рисков
		автоматизированных	нарушения безопасности
		информационных	телекоммуникационных
		систем и систем	систем и сетей.
		обеспечения	Уметь: применять
		информационной	средства защиты
		безопасности	информации в
			соответствии с
			эксплуатационной
			документацией, применять
			известные методики
			оценки угроз, принимать
			технические меры,
			направленные на
			повышение защищенности
			и снижения рисков
			нарушения безопасности
			телекоммуникационных систем.
			владеть: навыками
			эксплуатации средств
			защиты информации и
			анализа защищенности
			телекоммуникационных

		T :	T	
	не 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 компетенций	
компетенции	компетенции	за практикой		
			систем и сетей, методами проведения анализа угроз	
			информационной безопасности.	
ОПК-2	Способен	ОПК-2.1;	Знать:	
OTIK 2	разрабатывать	Выбирает методы	- технологии повышения	
	технический проект	решения задач для	защищенности	
	системы (подсистемы	защиты информации	распределенных	
	либо компонента	компьютерных систем	информационных систем;	
	системы) обеспечения	и сетей и систем	Уметь:	
	информационной	обеспечения	- выполнять определять	
	безопасности	информационной	характер угрозы и	
	осзопасности	безопасностью	масштабы последствий;	
		осзопасностью	- проектировать регламент	
			защищенного	
			взаимодействия	
			компонентов ТЛК	
			системы;	
			- минимизировать	
			последствия ущерба за	
			счет интеграции средств	
			защиты.	
			Владеть (или Иметь	
			опыт деятельности):	
			- навыками разработки	
			компонентов ТЛК систем;	
			- навыками обеспечения	
			совместимого	
			взаимодействия отдельных	
			модулей;	
		ОПК-2.2;	Знать: основные признаки	
		Разрабатывает тестовые	возникновения ошибок в	
		планы и сценарии	телекоммуникационных	
		тестирования	системах и сетях	
		разработанного	<i>Уметь:</i> в процессе	
		средства обеспечения	эксплуатации фиксировать	
		информационной	режимы работы в	
		безопасности	телекоммуникационных	
			системах и сетях,	
			отличные от штатных	
			Владеть (или Иметь	
			опыт деятельности):	
			навыками обнаружения	
			сбоев и отказов в в	

	разрабатывать проекты организационно-	Проводит технико- экономическое	- основы формирования исходных данных для
ОПК-3	Способен	ОПК-2.4; Определяет характеристики систем защиты информации	информации. Знать состав и функциональные возможности средств защиты информации телекоммуникационной системы. Уметь: совершенствовать состав и функциональные возможности средств защиты информации телекоммуникационной системы Владеть (или Иметь опыт деятельности): навыками оценки функциональных возможностей средств защиты информации телекоммуникационной системы Знать:
компетенции	компетенции	за практикой ОПК-2.3; Проектирует подсистемы безопасности информационных систем с учетом действующих нормативных и методических документов	телекоммуникационных системах и сетях Знать правовые нормы и стандарты для разработки инструкций, регламентов, положений и приказов, регламентирующих защиту информации Уметь: составлять проекты инструкций, регламентов, положений и приказов, регламентов, положений и приказов, регламентор доступа в организации Владеть (или Иметь опыт деятельности): навыками организации документооборота в области защиты
код	а практикой) наименование компетениии	компетенции, закрепленного за практикой	индикаторами достижения компетенций
Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные		Код и наименование индикатора достижения	Планируемые результаты обучения по практике, соотнесенные с

Планипуемы		Код	Планируемые	
Планируемые результаты освоения основной профессиональной		и наименование	результаты обучения	
образовательной программы		и наименование индикатора	по практике,	
(компетенции, закрепленные		достижения	соотнесенные с	
за практикой)		компетенции,	индикаторами	
код	наименование	закрепленного	достижения компетенций	
компетенции	компетенции	за практикой	ooemusicenusi kosmemeniiiii	
Komitemeniquu	распорядительных	обоснование проектных	телекоммуникационных	
	документов по	решений в области	задач;	
	обеспечению	построения систем	- основы экономического	
	информационной	обеспечения	обоснования проекта.	
	безопасности	информационной	Уметь:	
		безопасности	- анализировать исходные	
			данные для обоснования	
			целесообразности	
			разработки проекта;	
			- анализировать	
			предметную область и	
			создавать декларативное	
			описание задачи;	
			- применять принципы	
			выявления ключевых	
			параметров работы	
			информационной системы;	
			Владеть (или Иметь	
			опыт деятельности):	
			- приемами анализа	
			полноты и корректности	
			ключевых параметров	
		ОПК-3.2;	эксплуатации;	
		,	Знать: каналы утечки конфиденциальной	
		Рассчитывает риски информационной	1 '''	
		безопасности		
		Осзопасности	техническим каналам, основные тактико-	
			технические	
			характеристики, принципы	
			построения технических	
			средств передачи и защиты	
			информации, виды	
			сигналов и способы	
			распространения,	
			принципы и способы	
			организации системы	
			защиты информации на	
			объектах информатизации.	
			Уметь: Осуществлять	
			эксплуатацию технических	
			средств защиты	
			информации в	
			соответствии с	
			требованиями инструкций,	

Планируемые результаты освоения		Код	Планируемые
основной профессиональной		и наименование	результаты обучения
образовательной программы		индикатора	по практике,
(компетені	ции, закрепленные	достижения	соотнесенные с
за п	ірактикой)	компетенции,	индикаторами
код	наименование	закрепленного	достижения компетенций
компетенции	компетенции	за практикой	
	,		эксплуатационной
			документации.
			Владеть: навыками
			оценки рисков, связанных
			с осуществлением угроз
			безопасности.
		ОПК-3.3;	Знать:
		Выбирает	- технологии повышения
		инструментарий в	защищенности
		области	распределенных
		проектирования и	информационных систем;
		управления	Уметь:
		информационной	- выполнять определять
		безопасности	характер угрозы и
			масштабы последствий;
			- проектировать регламент
			защищенного
			взаимодействия
			компонентов ТЛК
			системы;
			- минимизировать
			последствия ущерба за
			счет интеграции средств
			защиты.
			Владеть (или Иметь
			опыт деятельности):
			- навыками разработки
			компонентов ТЛК систем;
			- навыками обеспечения
			совместимого
			взаимодействия отдельных
			модулей;

основной образоват (компете	е результаты освоения и профессиональной тельной программы гнции, закрепленные и практикой) наименование компетенции	Код и наименование индикатора достижения компетенции, закрепленного за практикой ОПК-3.4; Разрабатывает организационно- распорядительную документацию по обеспечению информационной безопасности	Планируемые результаты обучения по практике, соотнесенные с индикаторами достижения компетенций Знать основные требования, предъявляемые к организации защиты информации ограниченного доступа угрозы безопасности и модели нарушителя объекта информатизации Уметь: разрабатывать требования, предъявляемые к
		организационно-	предъявляемые к
		документацию по обеспечению информационной	информации ограниченного доступа угрозы безопасности и модели нарушителя объекта информатизации <i>Уметь:</i> разрабатывать требования,
		ОПК-3.5; Разрабатывает модели угроз и нарушителей информационной безопасности информационных систем	Знать основные угрозы безопасности и модели нарушителя объекта информатизации Уметь: разрабатывать модели угроз и модели нарушителя объекта информатизации Владеть (или Иметь опыт деятельности): навыками оценки угроз для объекта информатизации

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» профессиональной образовательной программы – магистратура Информационная безопасность, профиль «Защищенные информационные системы». Практика проходит на 1 курсе во 2 семестре.

Объем производственной технологической практики, установленный учебным планом, – 6 зачетных единиц, продолжительность – 4 недели (216 часов).

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 24 часа (часы указаны в учебном плане в графе «Пр»), работа обучающегося в иных формах — 192 часов (часы указаны в учебном плане в графе «СР»).

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

№	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

Таблица 4 – Этапы и содержание практики

		университета;	
		4) информация о требованиях к	
		отчетным документам по	
		практике;	
		5) первичный инструктаж по	
_	0 "	технике безопасности.	00
2	Основной этап	Работа обучающихся в	80
0.1	n	профильной организации	2
2.1	Знакомство с	Знакомство с профильной	2
	профильной	организацией, руководителем	
	организацией	практики от организации,	
		рабочим местом и должностной	
		инструкцией.	_
		Инструктаж по технике	5
		безопасности на рабочем месте.	_
		Знакомство с содержанием	3
		деятельности профильной	
		организации по обеспечению	
		информационной безопасности и	
		проводимыми в нем	
		мероприятиями.	
		Изучение нормативных правовых	1
		актов профильной организации по	
		обеспечению информационной	
		безопасности (политика	
		безопасности профильной	
		организации, положения,	
		приказы, инструкции,	
		должностные обязанности,	
		памятки и др.).	
2.2	Практическая	Самостоятельное проведение	80.
	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 формулирования	
	профессиональной	предложений по	
	деятельностью)	совершенствованию системы	
	/	защиты информации в ТКС.	
		Создание плана работы	
		коллектива из 3 – 4 человек,	
	<u> </u>	TOTAL TO TOTAL TOT	

реализующего политику безопасности в ТКС обработка 15 Самостоятельная полученных систематизация данных средств c помощью проектирования И выполнения технико-экономических расчетов. Организация работы 2-3 человек и руководство их работой процессе обработки систематизации полученных данных. Представление результатов мониторинга руководителю практики от организации Самостоятельное проведение анализа результатов проведенного информационной мониторинга безопасности. Организация работы 2-3 человек и руководство работой ИΧ процессе работ по разработки систем защиты информации. эффективности Оценка применения средств информационной безопасности. Представление результатов анализа и обоснование оценки руководителю практики организации. Самостоятельная подготовка рекомендаций ПО повышению уровня информационной безопасности предприятия. Организация работы 2-3 человек и руководство их работой процессе подготовки рекомендаций повышению no информационной уровня безопасности предприятия. Представление своих рекомендаций руководителю

		практики от организации.	
3	Заключительный	Оформление дневника практики.	28
	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 технологической 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 оценки эффективности применения средств обеспечения информационной безопасности.
- Оценка соответствия рисков информационной безопасности ТКС применяемым технологиям.
- 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* формиров	Этапы* формирования компетенций и дисциплины (модули), практики,				
наименование	НИР, при изучении которых формируется данная компетенция					
компетенции	начальный основной завершающий					
1	2	3	4			
ОПК-1	Математическое моделирование технических систем	Производственная технологи	ическая практика			
ОПК-2	Управление разработкой систем безопасности	Методы и средства пространственного анализа Методы пространственного моделирования радиоканала	Производственная проектно-технологическая практика			
ОПК-3	Управление разработкой систем	Производственная проектно-	технологическая практика			

безопасности

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

Код	Лица 0.2 – 110к Показатели	казатели и критерии оценивания компетенций, шкала оценивания Критерии и шкала оценивания компетенций			
компетенц ии/ этап (указывает ся название этапа из n.6.1)	оценивания компетенций (индикаторы достижения компетенций , закрепленные за	Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)	
	практикой)				
1	2	3	4	5	
ОПК-1/ завершаю щий	ОПК-1.1 Проектируе т информаци онные системы с учетом различных технологий обеспечени я информаци онной безопасност и	Знать: основные угрозы информационной безопасности; Уметь: выявлять угрозы информационной безопасности; Владеть (или Иметь опыт деятельности): навыками классификации угроз;	Возможные каналы утечки конфиденциальной информации; Уметь: снижать вероятность отрицательных последствий сетевого взаимодействия; - классифицировать угрозы информационной безопасности; Владеть (или Иметь опыт деятельности): навыками выявления уязвимостей технических каналов связи информационных систем.	Знать: - основные угрозы информационной безопасности; - возможные каналы утечки конфиденциальной информации; - нормативноправовые аспекты обеспечения информационной безопасности РФ; Уметь: - выявлять угрозы информационной безопасности; - снижать вероятность отрицательных последствий сетевого взаимодействия; - классифицировать угрозы информационной безопасности; Владеть (или Иметь опыт деятельности): - навыками классификации угроз; - навыками выявления	

1	2	3	4	5
				уязвимостей
				технических
				каналов связи
				информационных
				систем.
	ОПК-1.2	<i>Знать:</i> критерии	<i>Знать:</i> методы	<i>Знать:</i> критерии
	Разрабатыва	оценки показателей	достижения	оценки показателей
	ет системы	моделируемых	целевых	моделируемых
	обеспечени	систем	показателей систем	систем, знать
	Я	Уметь:	Уметь:	методы достижения
	информаци	сопоставлять	сопоставлять	целевых
	онной	результаты	результаты	показателей систем
	безопасност	моделирования с	моделирования с	Уметь:
	и объекта	изменением	изменением	сопоставлять
		параметров	параметров	результаты
		моделирования	моделирования	моделирования с
		Владеть (или	Владеть (или	изменением
		Иметь опыт	Иметь опыт	параметров
		деятельности):	деятельности):	моделирования
		навыками	навыками	Владеть (или
		оптимизации	оптимизации	Иметь опыт
		параметров	параметров	деятельности):
		моделируемых	моделируемых	навыками
		систем	систем	оптимизации
				параметров
				моделируемых
	ОПК-1.3	2	2	систем
	Планирует	Знать	Знать	Знать
	и оценивает	методологию установления	методологию установления	методологию
	трудоёмкос	зависимостей	зависимостей	установления зависимостей
	ть проекта,	между	между	между параметрами
	включая	параметрами	параметрами	систем и
	техническое	систем.	систем и	показателями их
	, кадровое и	Уметь: изменять	показателями их	функционирования.
	финансовое	целевые	функционирования.	Уметь: изменять
	обеспечени	характеристики	Уметь:	целевые
	е, принятие	функционирования	настраивать	характеристики
	совместных	телекоммуникацио	целевые	функционирования
	решений	нных систем за	характеристики	телекоммуникацио
	1	счёт изменения	функционирования	нных систем за
		параметров их	телекоммуникацио	счёт изменения
		работы	нных систем	параметров их
		Владеть (или	Владеть (или	работы
		Иметь опыт	Иметь опыт	Владеть (или
		деятельности):	деятельности):	Иметь опыт
		научного	научного	деятельности):
		обоснования	обоснования	научного
		решений,	решений,	обоснования
		направленных	направленных	решений,
		улучшение	улучшение	направленных

1	2	3	4	5
		существующих методов защиты информации	существующих методов защиты информации	улучшение существующих методов защиты информации
	ОПК-1.4 Формирует актуальную модель угроз для автоматизир ованных информаци онных систем и учитывает её положения при формирован ии требований техническог о задания на проектируе мую систему обеспечени я информаци онной безопасност и	Знать: Правовые нормы и стандарты по защите конфиденциальной информации при эксплуатации телекоммуникацио нной системы. Уметь: применять существующий инструментарий программных и аппаратных средств. Владеть (или Иметь опыт деятельности): навыками работы с программными и аппаратными средствами телекоммуникацио нной системы	Знать: Правовые нормы и стандарты по защите конфиденциальной информации при эксплуатации телекоммуникацио нной системы. Уметь: применять существующий инструментарий программных и аппаратных средств при эксплуатации телекоммуникацио нной системы. Владеть (или Иметь опыт деятельности): навыками работы с программными и аппаратными средствами телекоммуникацио нной системы	Знать: Правовые нормы и стандарты по защите конфиденциальной информации при эксплуатации телекоммуникацио нной системы. Уметь: применять существующий инструментарий программных и аппаратных средств при эксплуатации телекоммуникацио нной системы, в том числе в защищённом исполнении Владеть (или Иметь опыт деятельности): навыками работы с программными и аппаратными средствами телекоммуникацио нной системы

1	2	3	4	5
	ОПК-1.5	<i>Знать:</i> комплекс	<i>Знать:</i> комплекс	<i>Знать:</i> комплекс
	Разрабатыва	мероприятий,	мероприятий,	мероприятий,
	ет	направленных на	технических мер и	технических мер и
	концептуал	повышение	методов,	методов,
	ьные	защищенности.	направленных на	направленных на
	стратегии	Уметь: применять	повышение	повышение
	решения	средства защиты	защищенности.	защищенности и
	задач	информации в	<i>Уметь:</i> применять	снижения рисков
	моделирова	соответствии с	известные	нарушения
	ния и	эксплуатационной	методики оценки	безопасности
	проектиров	документацией.	угроз, принимать	телекоммуникацио
	ания	Владеть:	технические меры,	нных систем и
	автоматизир	навыками	направленные на	сетей.
	ованных	эксплуатации	повышение	<i>Уметь:</i> применять
	информаци	средств защиты	защищенности и	средства защиты
1	онных	информации.	снижения рисков	информации в
	систем и	- -	нарушения	соответствии с
	систем		безопасности	эксплуатационной
	обеспечени		телекоммуникацио	документацией,
	Я		нных систем.	применять
	информаци		Владеть:	известные
	онной		навыками анализа	методики оценки
	безопасност		защищенности	угроз, принимать
	И		телекоммуникацио	технические меры,
			нных систем и	направленные на
			сетей.	повышение
				защищенности и
				снижения рисков
				нарушения
				безопасности
				телекоммуникацио
				нных систем.
				Владеть:
				навыками
				эксплуатации
				средств защиты
				информации и
				анализа
				защищенности
				телекоммуникацио
				нных систем и
				сетей, методами
				проведения анализа
				угроз
				информационной
				безопасности.
	ОПК-2.1	Знать:	Знать:	Знать:
	Выбирает	технологии	технологии	технологии
	методы	повышения	повышения	повышения
	решения	защищенности	защищенности	защищенности
	задач для	распределенных	распределенных	распределенных

1	2	3	4	5
	защиты	информационных	информационных	информационных
	информаци	систем;	систем;	систем;
	И	Уметь:	Уметь:	Уметь:
	компьютерн	выполнять	- проектировать	- ВЫПОЛНЯТЬ
	ых систем и	определять	регламент	определять
	сетей и	характер угрозы и	защищенного	характер угрозы и
	систем	масштабы	взаимодействия	масштабы
	обеспечени	последствий;	компонентов ТЛК	последствий;
	Я	Владеть (или	системы;	- проектировать
	информаци	Иметь опыт	Владеть (или	регламент
	онной	деятельности):	Иметь опыт	защищенного
	безопасност	- навыками	деятельности):	взаимодействия
	ью	разработки	- навыками	компонентов ТЛК
	ыо	компонентов ТЛК	обеспечения	системы;
		систем;	совместимого	- минимизировать
		O110101v1,	взаимодействия	последствия
			отдельных	ущерба за счет
			отдельных модулей;	интеграции средств
			модулен,	защиты.
				Владеть (или
				Иметь опыт
				деятельности):
				- навыками
				разработки
				компонентов ТЛК
				систем;
				- навыками
				обеспечения
				совместимого
				взаимодействия
				отдельных
				модулей;
				тодулен,
	ОПК-2.2	<i>Знать:</i> основные	<i>Знать:</i> методы и	<i>Знать:</i> основные
	Разрабатыва	признаки	средства	признаки
	ет тестовые	возникновения	устранения ошибок	возникновения
	планы и	ошибок в	В	ошибок в
	сценарии	телекоммуникацио	телекоммуникацио	телекоммуникацио
	тестировани	нных системах и	нных системах и	нных системах и
	Я	сетях	сетях	сетях
	разработанн	Уметь: в процессе	Уметь:	Уметь: в процессе
	ого	эксплуатации	в процессе	эксплуатации
	средства	фиксировать	эксплуатации	фиксировать
	обеспечени	режимы работы в	фиксировать	режимы работы в
	Я	телекоммуникацио	режимы работы в	телекоммуникацио
	информаци	нных системах и	телекоммуникацио	нных системах и
	онной	сетях, отличные от	нных системах и	сетях, отличные от
	безопасност	штатных	сетях, отличные от	штатных;
	И	Владеть (или	штатных;	анализировать
		Иметь опыт	анализировать	полученные данные
		деятельности):	полученные	анализировать

1	2	3	4	5
		навыками	данные	полученные данные
		обнаружения сбоев	Владеть (или	Владеть (или
		и отказов в	Иметь опыт	Иметь опыт
		телекоммуникацио	деятельности):	деятельности):
		нных системах и	навыками	навыками
		сетях	обнаружения сбоев	обнаружения сбоев
			и отказов в	и отказов в
			телекоммуникацио	телекоммуникацио
			нных системах и	нных системах и
			сетях	сетях
	ОПК-2.3	<i>Знать</i> правовые	<i>Знать</i> правовые	<i>Знать</i> правовые
	Проектируе	нормы для	стандарты для	нормы и стандарты
	Т	разработки	разработки	для разработки
	подсистемы	инструкций,	инструкций,	инструкций,
	безопасност	регламентирующих	регламентов,	регламентов,
	И	защиту	положений и	положений и
	информаци	информации	приказов,	приказов,
	онных	Уметь: составлять	регламентирующих	регламентирующих
	систем с	проекты	защиту	защиту
	учетом	инструкций,	информации	информации
	действующ	регламентов,	Уметь: составлять	<i>Уметь:</i> составлять
	их	положений и	проекты	проекты
	нормативны	приказов,	инструкций,	инструкций,
	хи	регламентирующих	регламентов,	регламентов,
	методическ	защиту	положений и	положений и
	их	информации	приказов,	приказов,
	документов	ограниченного	регламентирующих	регламентирующих
	-	доступа в	защиту	защиту
		организации	информации	информации
		Владеть (или	ограниченного	ограниченного
		Иметь опыт	доступа в	доступа в
		деятельности):	организации	организации
		навыками	Владеть (или	Владеть (или
		организации	Иметь опыт	Иметь опыт
		документооборота	деятельности):	деятельности):
		в области защиты	навыками	навыками
		информации.	организации	организации
			документооборота	документооборота
			в области защиты	в области защиты
			информации.	информации.
	ОПК-2.4	Знать состав	Знать	Знать состав и
	Определяет	средств защиты	функциональные	функциональные
	характерист	информации	возможности	возможности
	ики систем	телекоммуникацио	средств защиты	средств защиты
	защиты	нной системы.	информации	информации
	информаци	Уметь:	телекоммуникацио	телекоммуникацио
	И	совершенствовать	нной системы.	нной системы.
		состав	Уметь:	Уметь:
		возможности	совершенствовать	совершенствовать
		средств защиты	функциональные	состав и
	•	· -	· -•	

1	2	3	4	5
		информации	возможности	функциональные
		телекоммуникацио	средств защиты	возможности
		нной системы	информации	средств защиты
		Владеть (или	телекоммуникацио	информации
		Иметь опыт	нной системы	телекоммуникацио
		деятельности):	Владеть (или	нной системы
		навыками оценки	Иметь опыт	Владеть (или
		функциональных	деятельности):	Иметь опыт
		возможностей	навыками оценки	деятельности):
		средств защиты	функциональных	навыками оценки
		информации	возможностей	функциональных
		телекоммуникацио	средств защиты	возможностей
		нной системы	информации	средств защиты
			телекоммуникацио	информации
			нной системы	телекоммуникацио
ОПК-3/	OHIC 2.1	2	2	нной системы
завершаю	ОПК-3.1	Знать:	Знать:	Знать:
щий	Проводит	ОСНОВЫ	основы	- основы
	технико-	формирования	экономического обоснования	формирования исходных данных
	экономичес кое	исходных данных для	проекта.	исходных данных для
	обосновани	телекоммуникацио	проекта. Уметь:	телекоммуникацио
	е проектных	нных задач;	анализировать	нных задач;
	решений в	Уметь:	предметную	- основы
	области	анализировать	область и создавать	экономического
	построения	исходные данные	декларативное	обоснования
	систем	для обоснования	описание задачи;	проекта.
	обеспечени	целесообразности	Владеть (или	Уметь:
	Я	разработки	Иметь опыт	применять
	информаци	проекта;	деятельности):	принципы
	онной	Владеть (или	- приемами анализа	выявления
	безопасност	Иметь опыт	корректности	ключевых
	И	деятельности):	ключевых	параметров работы
		приемами анализа	параметров	информационной
		полноты ключевых	эксплуатации;	системы;
		параметров		Владеть (или
		эксплуатации;		Иметь опыт
				деятельности):
				- приемами анализа
				полноты и
				корректности
				ключевых
				параметров
	ОПК-3.2	Знать:	Знать:	эксплуатации; Знать: каналы
	Рассчитыва	каналы утечки	принципы	утечки
	ет риски	каналы утсчки конфиденциальной	построения	конфиденциальной
	информаци	информации по	технических	информации по
	онной	техническим	средств передачи и	техническим
	безопасност	каналам, основные	защиты	каналам, основные
	И	тактико-		тактико-
			информации, виды	

1	2	3	4	5
		технические	сигналов и способы	технические
		характеристики	распространения,	характеристики,
		Уметь:	принципы и	принципы
		Осуществлять	способы	построения
		эксплуатацию	организации	технических
		технических	системы защиты	средств передачи и
		средств защиты	информации на	защиты
		информации в	объектах	информации, виды
		соответствии с	информатизации.	сигналов и способы
		требованиями	Уметь:	распространения,
		инструкций,	Осуществлять	принципы и
		эксплуатационной	эксплуатацию	способы
		документации.	технических	организации
		Владеть:	средств защиты	системы защиты
		навыками оценки	информации в	информации на
		рисков, связанных	соответствии с	объектах
		с осуществлением	требованиями	информатизации.
		угроз безопасности.	инструкций,	Уметь:
			эксплуатационной	Осуществлять
			документации.	эксплуатацию
			Владеть:	технических
			навыками оценки	средств защиты
			рисков, связанных	информации в
			с осуществлением	соответствии с
			угроз безопасности.	требованиями
				инструкций,
				эксплуатационной
				документации.
				Владеть:
				навыками оценки
				рисков, связанных с
				осуществлением
	ОПК-3.3	2	2	угроз безопасности.
	Выбирает	Знать:	Знать:	Знать:
	инструмент	технологии повышения	методы повышения защищенности	методы и средства повышения
	арий в	защищенности	распределенных	защищенности
	арии в области	распределенных	информационных	распределенных
	проектиров	информационных	систем;	информационных
	ания и	систем;	Уметь:	систем;
	управления	Уметь:	проектировать	Уметь:
	информаци	выполнять	регламент	- выполнять
	онной	определять	защищенного	определять
	безопасност	характер угрозы и	взаимодействия	характер угрозы и
	И	масштабы	компонентов ТЛК	масштабы
		последствий;	системы;	последствий;
		Владеть (или	Владеть (или	- проектировать
		Иметь опыт	Иметь опыт	регламент
		деятельности):	деятельности):	защищенного
		навыками	навыками	взаимодействия
		разработки	обеспечения	компонентов ТЛК

1	2	3	4	5
		компонентов ТЛК	совместимого	системы;
		систем;	взаимодействия	- минимизировать
			отдельных	последствия
			модулей;	ущерба за счет
				интеграции средств
				защиты.
ļ				Владеть (или
ļ				Иметь onыm
ļ				деятельности):
ļ				- навыками
				разработки
				компонентов ТЛК
ļ				систем;
ļ				- навыками
ļ				обеспечения
				совместимого
				взаимодействия
				отдельных
				модулей;

1	2	3	4	5
	ОПК-3.4 Разрабатыва ет организаци онно-распорядите льную документац ию по обеспечени ю информаци онной безопасност и	Знать основные требования, предъявляемые к организации защиты информации ограниченного доступа Уметь: разрабатывать требования, предъявляемые к организации защиты информации ограниченного доступа Владеть (или Иметь опыт деятельности): навыками формулирования основных требований, предъявляемых к организации защиты информации ограниченного доступа	Знать угрозы безопасности и модели нарушителя объекта информатизации Уметь: разрабатывать требования, предъявляемые к организации информации ограниченного доступа Владеть (или Иметь опыт деятельности): навыками формулирования основных требований, предъявляемых к организации защиты информации ограниченного доступа	Знать основные требования, предъявляемые к организации защиты информации ограниченного доступа угрозы безопасности и модели нарушителя объекта информатизации Уметь: разрабатывать требования, предъявляемые к организации защиты информации ограниченного доступа Владеть (или Иметь опыт деятельности): навыками формулирования основных требований, предъявляемых к организации защиты информации ограниченного доступа
	ОПК-3.5 Разрабатыва ет модели угроз и нарушителе й	Знать основные угрозы безопасности объекта информатизации Уметь:	Знать основные модели нарушителя объекта информатизации Уметь: разрабатывать	Знать основные угрозы безопасности и модели нарушителя объекта информатизации

1	2	3	4	5	
	информаци	разрабатывать	модели нарушителя	Уметь:	
	онной	модели угроз	объекта	разрабатывать	
	безопасност	объекта	информатизации	модели угроз и	
	И	информатизации	Владеть (или	модели нарушителя	
	информаци	Владеть (или	Иметь опыт	объекта	
	онных	Иметь опыт	деятельности):	информатизации	
	систем	деятельности):	навыками оценки	Владеть (или	
		навыками оценки	угроз для объекта	Иметь опыт	
		угроз для объекта	информатизации	деятельности):	
		информатизации		навыками оценки	
				угроз для объекта	
				информатизации	

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)

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)				
ОПК-1	Дневник практики.			
завершающий	Отчёт по практике с научно-обоснованными решениями по			
	увеличению защищённости телекоммуникационных систем и			
	сетей			
	Доклад обучающегося на промежуточной аттестации (защита			
	отчета о практике).			
	Характеристика руководителя практики от организации			
	управленческих качеств обучающегося.			
ОПК-2	Дневник практики.			
завершающий	Отчет 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): Сформируйте 4 критерия эффектвиности			
	применения средств обеспечения ИБ в ТКС, произведите			
	шкалирование критериев и сформируйте итоговую оценку			
	эффективнсти использованных на рельном объекте решений.			
	Ответы на вопросы по содержанию практики на промежуточной			

	аттестации.
ОПК-3	Дневник практики.
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): Исходя из сформированных критериев предложите проектные, организационные и иные решения для повышения эффективности системы защиты. Доклад обучающегося на промежуточной аттестации (защита отчета о практике). Характеристика руководителя практики от организации 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

No	Предмет оценки	Критерии оценки	Максимальный балл
1	Содержание отчета 10 баллов	Достижение цели и выполнение задач практики в полном объеме	1
		Отражение в отчете всех предусмотренных программой практики видов работ, связанных с будущей профессиональной деятельностью	1
		Владение актуальными нормативными правовыми документами и профессиональной терминологией	1
		Соответствие структуры и содержания отчета требованиям, установленным в п. 5 настоящей	1

	T	T	1
		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	
1		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	2
		использования профессиональной	
		терминологии	
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		
		1	ı

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

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, Аудит информационной В. И. безопасности [Электронный ресурс]: учебное пособие для вузов / В. И. Аверченков. - 3-е стереотип. M. Флинта, 2016. 269 URL: изд., 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>К</u>омпания «Консультант Плюс» [официальный сайт]. 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 ИЛИ организации. 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 OB3.

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	Дат а	для изменения и подпись лица, проводившег о изменения
							и изменения