МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:
И.о. декана факультета ФиПИ
_____ Таныгин М.О.
(подпись, инициалы, фамилия)
«30» 08 2022 г.

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 обучения *очная*
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. кафедрой _____ Таныгин М.О.

Разработчик программы

к.т.н., доцент _____ Таныгин М.О.

(ученая степень и ученое звание, Ф.И.О.)

Директор научной библиотеки _____ Макаровская В.Г.

Рабочая программа практики пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, профиль «Защищенные информационные системы», одобренного Ученым советом университета протокол №7 «28» 02 20 22 г., на заседании кафедры ИБ протокол №1 от 30.08.22 .

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа практики пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, профиль «Защищенные информационные системы», одобренного Ученым советом университета протокол №7 «28» 02 20 22 г., на заседании кафедры ИБ протокол №1 от 30.08.2023 .

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа практики пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, профиль «Защищенные информационные системы», одобренного Ученым советом университета протокол №__ «___» _____ 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 и опыта профессиональной деятельности в области проектирования и реализации технологий информационной безопасности.

1.2. Задачи практики

1. Формирование профессиональных компетенций, установленных ФГОС ВО и закрепленных учебным планом за производственной проектно-технологической 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

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за практикой)		*Код и наименование индикатора достижения компетенции, закрепленного за практикой*	*Планируемые результаты обучения по практике, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
ОПК-1	Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	ОПК-1.1; Проектирует информационные системы с учетом различных технологий обеспечения информационной безопасности	***Знать:*** - основные угрозы информационной безопасности; - возможные каналы утечки конфиденциальной информации; - 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

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за практикой)		*Код и наименование индикатора достижения компетенции, закрепленного за практикой*	*Планируемые результаты обучения по практике, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			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 систем
		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 формировании	***Знать:*** Правовые нормы и стандарты по защите конфиденциальной информации при эксплуатации телекоммуникационной системы. ***Уметь:*** применять

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за практикой)		*Код и наименование индикатора достижения компетенции, закрепленного за практикой*	*Планируемые результаты обучения по практике, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
		требований технического задания на проектируемую систему обеспечения информационной безопасности	существующий инструментарий программных и аппаратных средств при эксплуатации 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; Разрабатывает концептуальные стратегии решения задач моделирования и проектирования автоматизированных информационных систем и систем обеспечения информационной безопасности	***Знать:*** комплекс мероприятий, технических мер и методов, направленных на повышение защищенности и снижения рисков нарушения безопасности телекоммуникационных систем и сетей. ***Уметь:*** применять средства защиты 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

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за практикой)		*Код и наименование индикатора достижения компетенции, закрепленного за практикой*	*Планируемые результаты обучения по практике, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			систем и сетей, методами проведения анализа угроз информационной безопасности.
ОПК-2	Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	ОПК-2.1; Выбирает методы решения задач для защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью	***Знать:*** - технологии повышения защищенности распределенных информационных систем; ***Уметь:*** - выполнять определять 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;
		ОПК-2.2; Разрабатывает тестовые планы и сценарии тестирования разработанного средства обеспечения информационной безопасности	***Знать:*** основные признаки возникновения ошибок в телекоммуникационных системах и сетях ***Уметь:*** в процессе эксплуатации фиксировать режимы работы в телекоммуникационных системах и сетях, отличные от штатных ***Владеть (****или* ***Иметь опыт деятельности):*** навыками обнаружения сбоев и отказов в в

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за практикой)		*Код и наименование индикатора достижения компетенции, закрепленного за практикой*	*Планируемые результаты обучения по практике, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			телекоммуникационных системах и сетях
		ОПК-2.3; Проектирует подсистемы безопасности информационных систем с учетом действующих нормативных и методических документов	***Знать*** правовые нормы и стандарты для разработки инструкций, регламентов, положений и приказов, регламентирующих защиту информации ***Уметь:*** составлять проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации ***Владеть (***или ***Иметь опыт деятельности):*** навыками организации документооборота в области защиты информации.
		ОПК-2.4; Определяет характеристики систем защиты 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
ОПК-3	Способен разрабатывать проекты организационно-	ОПК-3.1; Проводит технико-экономическое	***Знать:*** - основы формирования исходных данных для

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за практикой)		*Код и наименование индикатора достижения компетенции, закрепленного за практикой*	*Планируемые результаты обучения по практике, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
	распорядительных документов по обеспечению информационной безопасности	обоснование проектных решений в области построения систем обеспечения информационной безопасности	телекоммуникационных задач; - основы экономического обоснования проекта. ***Уметь:*** - 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 эксплуатации;
		ОПК-3.2; Рассчитывает риски информационной безопасности	***Знать:*** каналы утечки конфиденциальной информации по 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 основной профессиональной образовательной программы (компетенции, закрепленные за практикой)		*Код и наименование индикатора достижения компетенции, закрепленного за практикой*	*Планируемые результаты обучения по практике, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			эксплуатационной документации. ***Владеть:*** навыками оценки рисков, связанных с осуществлением угроз безопасности.
		ОПК-3.3; Выбирает инструментарий в области проектирования и управления информационной безопасности	***Знать:*** - технологии повышения защищенности распределенных информационных систем; ***Уметь:*** - выполнять определять 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;

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за практикой)		*Код и наименование индикатора достижения компетенции, закрепленного за практикой*	*Планируемые результаты обучения по практике, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
		ОПК-3.4; Разрабатывает организационно-распорядительную документацию по обеспечению информационной безопасности	***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; 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 в часть, формируемую участниками образовательных отношений, блока 2 «Практика» профессиональной образовательной программы – магистратура 10.04.01 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.

Таблица 4 – Этапы и содержание практики

№ п/п	Этапы практики	Содержание практики	Трудоемкость (час)
1	Подготовительный этап	Решение организационных вопросов: 1) распределение обучающихся по местам практики; 2) знакомство с целью, задачами, программой, порядком прохождения практики; 3) получение заданий от руководителя практики от	2

		университета; 4) информация о требованиях к отчетным документам по практике; 5) первичный инструктаж по технике безопасности.	
2	Основной этап	Работа обучающихся в профильной организации	80
2.1	Знакомство с профильной организацией	Знакомство с профильной организацией, руководителем практики от организации, рабочим местом и должностной инструкцией.	2
		Инструктаж по технике безопасности на рабочем месте.	5
		Знакомство с содержанием деятельности профильной организации по обеспечению информационной безопасности и проводимыми в нем мероприятиями.	3
		Изучение нормативных правовых актов профильной организации по обеспечению информационной безопасности (политика безопасности профильной организации, положения, приказы, инструкции, должностные обязанности, памятки и др.).	1
2.2	Практическая подготовка обучающихся *(непосредственное выполнение обучающимися видов работ, связанных с будущей профессиональной деятельностью)*	Самостоятельное проведение мониторинга и (или) производственного контроля эффективности применения средств защиты информации в ТКС. Организация работы 2-3 человек и руководство их работой в процессе формулирования предложений по совершенствованию системы защиты информации в ТКС. Создание плана работы коллектива из 3 – 4 человек,	80.

		реализующего политику безопасности в ТКС	
		Самостоятельная обработка и систематизация полученных данных с помощью средств проектирования и выполнения технико-экономических расчетов. *Организация работы 2-3 человек и руководство их работой в процессе обработки и систематизации полученных данных.* Представление результатов мониторинга руководителю практики от организации	15
		Самостоятельное проведение анализа результатов проведенного мониторинга информационной безопасности. Организация работы 2-3 человек и руководство их работой в процессе работ по разработки систем защиты информации. Оценка эффективности применения средств 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.	
3	Заключительный этап	Оформление дневника практики.	28
		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 наименование компетенции	Этапы* формирования компетенций и дисциплины (модули), практики, НИР, при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
ОПК-1	Математическое моделирование технических систем	Производственная технологическая 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 компетенции/ этап *(указывается название этапа из п.6.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за практикой)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно»)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
ОПК-1/ завершающий	ОПК-1.1 Проектирует информационные системы с учетом различных технологий обеспечения информационной безопасности	***Знать:*** основные угрозы информационной безопасности; ***Уметь:*** выявлять угрозы информационной безопасности; ***Владеть (****или* ***Иметь опыт деятельности):*** навыками классификации угроз ;	***Знать:*** 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; - 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

1	2	3	4	5
				уязвимостей технических каналов связи информационных систем.
	ОПК-1.2 Разрабатывает системы обеспечения информационной безопасности объекта	***Знать:*** критерии оценки показателей моделируемых систем ***Уметь:*** сопоставлять результаты моделирования с изменением параметров моделирования ***Владеть (****или* ***Иметь опыт деятельности):*** навыками оптимизации параметров 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 систем	***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 систем
	ОПК-1.3 Планирует и оценивает трудоёмкость проекта, включая техническое, кадровое и финансовое обеспечение, принятие совместных решений	***Знать*** методологию установления зависимостей между параметрами систем. ***Уметь:*** изменять целевые характеристики функционирования телекоммуникационных систем за счёт изменения параметров их работы ***Владеть (****или* ***Иметь опыт деятельности):*** научного обоснования решений, направленных улучшение	***Знать*** методологию установления зависимостей между параметрами систем и показателями их функционирования. ***Уметь:*** настраивать целевые характеристики функционирования телекоммуникационных систем ***Владеть (****или* ***Иметь опыт деятельности):*** научного обоснования решений, направленных улучшение	***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

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 автоматизированных информационных систем и учитывает её положения при формировании требований технического задания на проектируемую систему обеспечения информационной безопасности	***Знать:*** Правовые нормы и стандарты по защите конфиденциальной информации при эксплуатации телекоммуникационной системы. ***Уметь:*** применять существующий инструментарий программных и аппаратных средств. ***Владеть (****или* ***Иметь опыт деятельности):*** навыками работы с программными и аппаратными средствами телекоммуникационной системы	***Знать:*** Правовые нормы и стандарты по защите конфиденциальной информации при эксплуатации телекоммуникационной системы. ***Уметь:*** применять существующий инструментарий программных и аппаратных средств при эксплуатации телекоммуникационной системы. ***Владеть (****или* ***Иметь опыт деятельности):*** навыками работы с программными и аппаратными средствами телекоммуникационной системы	***Знать:*** Правовые нормы и стандарты по защите конфиденциальной информации при эксплуатации телекоммуникационной системы. ***Уметь:*** применять существующий инструментарий программных и аппаратных средств при эксплуатации телекоммуникационной системы, в том числе в защищённом исполнении ***Владеть (****или* ***Иметь опыт деятельности):*** навыками работы с программными и аппаратными средствами телекоммуникационной системы

1	2	3	4	5
	ОПК-1.5 Разрабатывает концептуальные стратегии решения задач моделирования и проектирования автоматизированных информационных систем и систем обеспечения информационной безопасности	***Знать:*** комплекс мероприятий, направленных на повышение защищенности. ***Уметь:*** применять средства защиты информации в соответствии с эксплуатационной документацией. ***Владеть:*** навыками эксплуатации средств защиты информации.	***Знать:*** комплекс мероприятий, технических мер и методов, направленных на повышение защищенности. ***Уметь:*** применять известные методики оценки угроз, принимать технические меры, направленные на повышение защищенности и снижения рисков нарушения безопасности телекоммуникационных систем. ***Владеть:*** навыками анализа защищенности телекоммуникационных систем и сетей.	***Знать:*** комплекс мероприятий, технических мер и методов, направленных на повышение защищенности и снижения рисков нарушения безопасности телекоммуникационных систем и сетей. ***Уметь:*** применять средства защиты 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 систем и сетей, методами проведения анализа угроз информационной безопасности.
ОПК-2 завершающий	ОПК-2.1 Выбирает методы решения задач для	***Знать:*** технологии повышения защищенности распределенных	***Знать:*** технологии повышения защищенности распределенных	***Знать:*** технологии повышения защищенности распределенных

1	2	3	4	5
	защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью	информационных систем; ***Уметь:*** выполнять определять характер угрозы и масштабы последствий; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками разработки компонентов ТЛК систем;	информационных систем; ***Уметь:*** - проектировать регламент защищенного взаимодействия компонентов ТЛК системы; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками обеспечения совместимого взаимодействия отдельных модулей;	информационных систем; ***Уметь:*** - выполнять определять 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;
	ОПК-2.2 Разрабатывает тестовые планы и сценарии тестирования разработанного средства обеспечения информационной безопасности и	***Знать:*** основные признаки возникновения ошибок в телекоммуникационных системах и сетях ***Уметь:*** в процессе эксплуатации фиксировать режимы работы в телекоммуникационных системах и сетях, отличные от штатных ***Владеть (****или* ***Иметь опыт деятельности):***	***Знать:*** методы и средства устранения ошибок в телекоммуникационных системах и сетях ***Уметь:*** в процессе эксплуатации фиксировать режимы работы в телекоммуникационных системах и сетях, отличные от штатных; анализировать полученные	***Знать:*** основные признаки возникновения ошибок в телекоммуникационных системах и сетях ***Уметь:*** в процессе эксплуатации фиксировать режимы работы в телекоммуникационных системах и сетях, отличные от штатных; анализировать полученные данные анализировать

1	2	3	4	5
		навыками обнаружения сбоев и отказов в телекоммуникационных системах и сетях	данные ***Владеть*** *(или* ***Иметь опыт деятельности):*** навыками обнаружения сбоев и отказов в телекоммуникационных системах и сетях	полученные данные ***Владеть*** *(или* ***Иметь опыт деятельности):*** навыками обнаружения сбоев и отказов в телекоммуникационных системах и сетях
	ОПК-2.3 Проектирует подсистемы безопасности информационных систем с учетом действующих нормативных и методических документов	***Знать*** правовые нормы для разработки инструкций, регламентирующих защиту информации ***Уметь:*** составлять проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации ***Владеть*** *(или* ***Иметь опыт деятельности):*** навыками организации документооборота в области защиты информации.	***Знать*** правовые стандарты для разработки инструкций, регламентов, положений и приказов, регламентирующих защиту информации ***Уметь:*** составлять проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации ***Владеть*** *(или* ***Иметь опыт деятельности):*** навыками организации документооборота в области защиты информации.	***Знать*** правовые нормы и стандарты для разработки инструкций, регламентов, положений и приказов, регламентирующих защиту информации ***Уметь:*** составлять проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации ***Владеть*** *(или* ***Иметь опыт деятельности):*** навыками организации документооборота в области защиты информации.
	ОПК-2.4 Определяет характеристики систем защиты информации	***Знать*** состав средств защиты информации телекоммуникационной системы. ***Уметь:*** совершенствовать состав возможности средств защиты	***Знать*** функциональные возможности средств защиты информации телекоммуникационной системы. ***Уметь:*** совершенствовать функциональные	***Знать*** состав и функциональные возможности средств защиты информации телекоммуникационной системы. ***Уметь:*** совершенствовать состав и

1	2	3	4	5
		информации телекоммуникационной системы ***Владеть (или Иметь опыт деятельности):*** навыками оценки функциональных возможностей средств защиты информации телекоммуникационной системы	возможности средств защиты информации телекоммуникационной системы ***Владеть (или Иметь опыт деятельности):*** навыками оценки функциональных возможностей средств защиты информации телекоммуникационной системы	функциональные возможности средств защиты информации телекоммуникационной системы ***Владеть (или Иметь опыт деятельности):*** навыками оценки функциональных возможностей средств защиты информации телекоммуникационной системы
ОПК-3/ завершающий	ОПК-3.1 Проводит технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности	***Знать:*** основы формирования исходных данных для телекоммуникационных задач; ***Уметь:*** анализировать исходные данные для обоснования целесообразности разработки проекта; ***Владеть (или Иметь опыт деятельности):*** приемами анализа полноты ключевых параметров эксплуатации;	***Знать:*** основы экономического обоснования проекта. ***Уметь:*** анализировать предметную область и создавать декларативное описание задачи; ***Владеть (или Иметь опыт деятельности):*** - приемами анализа корректности ключевых параметров эксплуатации;	***Знать:*** - основы формирования исходных данных для телекоммуникационных задач; - основы экономического обоснования проекта. ***Уметь:*** применять принципы выявления ключевых параметров работы информационной системы; ***Владеть (или Иметь опыт деятельности):*** - приемами анализа полноты и корректности ключевых параметров эксплуатации;
	ОПК-3.2 Рассчитывает риски информационной безопасности	***Знать:*** каналы утечки конфиденциальной информации по техническим каналам, основные тактико-	***Знать:*** принципы построения технических средств передачи и защиты информации, виды	***Знать:*** каналы утечки конфиденциальной информации по техническим каналам, основные тактико-

1	2	3	4	5
		технические характеристики ***Уметь:*** Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями инструкций, эксплуатационной документации. ***Владеть:*** навыками оценки рисков, связанных с осуществлением угроз безопасности.	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, эксплуатационной документации. ***Владеть:*** навыками оценки рисков, связанных с осуществлением угроз безопасности.	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, эксплуатационной документации. ***Владеть:*** навыками оценки рисков, связанных с осуществлением угроз безопасности.
	ОПК-3.3 Выбирает инструментарий в области проектирования и управления информационной безопасности	***Знать:*** технологии повышения защищенности распределенных информационных систем; ***Уметь:*** выполнять определять характер угрозы и масштабы последствий; ***Владеть (или Иметь опыт деятельности):*** навыками разработки	***Знать:*** методы повышения защищенности распределенных информационных систем; ***Уметь:*** проектировать регламент защищенного взаимодействия компонентов ТЛК системы; ***Владеть (или Иметь опыт деятельности):*** навыками обеспечения	***Знать:*** методы и средства повышения защищенности распределенных информационных систем; ***Уметь:*** - выполнять определять характер угрозы и масштабы последствий; - проектировать регламент защищенного взаимодействия компонентов ТЛК

1	2	3	4	5
		компонентов ТЛК систем;	совместимого взаимодействия отдельных модулей;	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;

1	2	3	4	5
	ОПК-3.4 Разрабатывает организационно-распорядительную документацию по обеспечению информационной безопасности	***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 защиты 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 Разрабатывает модели угроз и нарушителей	***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
	информационной безопасности информационных систем	разрабатывать модели угроз объекта информатизации ***Владеть (или Иметь опыт деятельности):*** навыками оценки угроз для объекта информатизации	модели нарушителя объекта информатизации ***Владеть (или Иметь опыт деятельности):*** навыками оценки угроз для объекта информатизации	***Уметь:*** разрабатывать модели угроз и модели нарушителя объекта информатизации ***Владеть (или Иметь опыт деятельности):*** 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 формирования компетенции в процессе освоения ОПОП ВО *(указывается название этапа из п.6.1)*	Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности
ОПК-1 завершающий	Дневник практики. 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 завершающий	Дневник практики. 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 эффективности 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 завершающий	Дневник практики. 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

№	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

		программы	
		Полнота и глубина раскрытия содержания разделов отчета	1
		Достоверность и достаточность приведенных в отчете данных	1
		Правильность выполнения расчетов и измерений	1
		Глубина анализа данных	1
		Обоснованность выводов и рекомендаций	1
		Самостоятельность при подготовке отчета	1
2	Оформление отчета 2 балла	Соответствие оформления отчета требованиям, установленным в п.5 настоящей программы	1
		Достаточность использованных источников	1
3	Содержание и оформление презентации (графического материала) 4 балла	Полнота и соответствие содержания презентации (графического материала) содержанию отчета	2
		Грамотность речи и правильность использования профессиональной терминологии	2
4	Ответы на вопросы о содержании практики, в том числе на вопросы о практической подготовке (видах работ, связанных с будущей профессиональной деятельностью, выполненных на практике) 4 балла	Полнота, точность, аргументированность ответов,	4

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 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:

4) Аверченков, В. И. Аудит информационной безопасности [Электронный ресурс] : учебное пособие для вузов / В. И. Аверченков. - 3-е изд., стереотип. - М. : Флинта, 2016. - 269 с. - 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. Компания «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 (м*ежсетевые 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:

м*ежсетевые 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 – ОВЗ) 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 ОВЗ 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 или работников профильной 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 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

Номер изменения	Номера страниц				Всего страниц	Дата	Основание для изменения и подпись лица, проводившего изменения
	изме-ненных	замененных	аннулированных	новых			