МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:
И.о. декана факультета фундаментальной и прикладной информатики
(наименование фта, полностью)
_____ Таныгин М.О.
(подпись, инициалы, фамилия)
«31» 08 2021 г.

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

Производственная проектно-технологическая практика

(наименование вида и типа практики)

ОПОП ВО 10.04.01 Информационная безопасность,
(шифр с наименованием направления подготовки (специальности))

«Защищённые информационные системы»
(наименование направленности (профиля) или специализации)

форма обучения очная
(очная, очно-заочная, заочная)

Курск – 20__

Рабочая программа практики составлена в соответствии с:

– федеральным государственным образовательным стандартом высшего образования – магистратура по направлению подготовки 10.04.01 Информационная безопасность, утвержденным приказом Минобрнауки России от 26 ноября 2020 г. № 1455;

– учебным планом ОПОП ВО 10.04.01 Информационная безопасность, профиль «Защищённые информационные системы», одобренным Ученым советом университета (протокол № 6 «22» февраля 2021 г.).

Рабочая программа практики обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 10.04.01 Информационная безопасность, профиль «Защищённые информационные системы» на заседании кафедры информационной безопасности «30» 08 2021 г., протокол № 6.

Зав. кафедрой _____ Таныгин М.О.

Разработчик программы
к.т.н., доцент _____ Ефремов М.А.

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 «Защищённые информационные системы», одобренного Ученым советом университета протокол №5 «26» 02 2021 г., на заседании кафедры ИБ №1 от 30.06.222.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой Таныгин М.О.

Рабочая программа практики пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, профиль «Защищённые информационные системы», одобренного Ученым советом университета протокол №7 «28» 02 2022 г., на заседании кафедры ИБ №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 «Защищённые 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 проектно-технологической практики является получение профессиональных умений и опыта профессиональной деятельности в области информационной безопасности в условиях реального производства.

1.2. Задачи практики

1. Формирование профессиональных компетенций, установленных ФГОС ВО и закрепленных учебным планом за производственной проектно-технологической практикой.
2. Освоение современных информационных технологий и профессиональных программных комплексов, применяемых в области информационной безопасности.
3. Совершенствование навыков подготовки, представления и защиты информационных, аналитических 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 – проектно-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 профилю 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 требо-

ваниям 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*		
ПК – 1	Способен формировать проектные решения по созданию и модернизации защищённых информационных систем	ПК – 1.1 Разрабатывает проектные документы на средства защиты информации создаваемых телекоммуникационных систем и сетей	***Знать:*** - нормативная база, регламентирующая создание средств защиты информации создаваемых телекоммуникационных систем и сетей; - назначение и классификация средств защиты информации; - источники и классификация угроз; - методы проектирования средств защиты информации создаваемых телекоммуникационных систем и сетей. ***Уметь:*** - разрабатывать проекты технических заданий на проектирование средств защиты информации; - разрабатывать проекты нормативно-распорядительные документов; - классифицировать и оценивать угрозы ИБ для объекта информатизации; - составлять проектную документацию на систему защиты информации. ***Владеть (или Иметь опыт деятельности):*** - навыками разработки технических заданий;

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*		
			- навыками разработки проектов нормативно-распорядительных документов; - навыками оценки угроз ИБ.
		ПК – 1.2 Готовит техническую и проектную документацию по вопросам создания защищённых информационных систем	***Знать:*** основные методы организационного обеспечения процесса подготовки документов, регламентирующих создание защищённых информационных систем; - организационные меры по защите информации; - нормативные правовые акты в области защиты информации. ***Уметь:*** - готовить проектную и техническую документацию по вопросам создания защищённых информационных систем; - готовить проекты методических документов; - применять необходимые нормативные правовые акты; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками организации проекта; - навыками подготовки необходимой технической и проектной документации;
		ПК – 1.3 Сопоставляет характеристики проектируемых решений с требованиями защиты информации	***Знать:*** - характеристики проектируемых решений; - нормативная база, регламентирующая создание средств защиты информации; ***Уметь:*** - анализировать характеристики проектируемых решений; - сопоставлять характеристики проектируемых решений с требованиями защиты информации; ***Владеть (или Иметь опыт деятельности):*** - навыками составления проектируемых решений;

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*		
			- навыками анализа характеристик проектируемых решений с требованиями защиты информации
		ПК – 1.4 Формирует конфигурацию и состав защищённых информационных систем	***Знать:*** - определение конфигурации; - состав защищённых информационных систем; - архитектура средств контроля конфигурации; - модули ***Уметь:*** - формировать эталон конфигурации ИС; - считывать текущую конфигурацию и сравнивать её с эталонной; ***Владеть (или Иметь опыт деятельности):*** - навыками анализа состава защищённых информационных систем; - навыками работы с конфигурационными файлами; - навыками работы с несколькими модулями проверки
ПК – 2	Способен организовать работы по выполнению требований защиты информации ограниченного доступа в защищённых информационных системах	ПК – 2.1 Управляет работой специалистов по созданию и эксплуатации средств защиты информации в защищённых информационных системах	**Знать:** - основные методы организационного обеспечения процесса подготовки документов, регламентирующих создание защищённых информационных систем; ***Уметь:*** - готовить проектную и техническую документацию по вопросам создания защищённых информационных систем; **Владеть (или Иметь опыт деятельности):** - навыками организации проекта
		ПК – 2.2 Формирует комплекс мер	***Знать:*** - основные целевые критерии для оценки

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*		
		(принципов, правил, процедур, практических приемов, методов, средств) для защиты в защищённых информационных системах	эффективности исследуемых систем; - определение информации и её типы с точки зрения защищённости ИС; - принципы создания экспертной комиссии для проведения оценки эффективности исследуемых систем с учётом основных типов угроз нарушения: конфиденциальности, целостности, доступности информации. ***Уметь:*** - определять целевые критерии для оценки эффективности исследуемых систем; - определять тип информации; - самостоятельно организовывать экспертную комиссию для оценивания эффективности исследуемых систем ***Владеть (или Иметь опыт деятельности):*** - навыками анализа целевых критериев для оценивания эффективности исследуемых систем; - навыками определения типа информации, подлежащей защите; - навыками организации экспертной оценки эффективности исследуемых систем.
		ПК – 2.3 Управляет процессом разработки моделей угроз и моделей нарушителя безопасности информационных систем	**Знать:** - структуру и функционал защищённых информационных систем; -требования стандартов информационной безопасности, предъявляемые к информационным системам в защищённом исполнении. **Уметь:** - анализировать структуру информационных систем и формулировать требования и технические регламенты для обеспечения их информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими до-

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*		
			кументами ФСБ России, ФСТЭК России; - организовывать эксплуатацию защищённых информационных систем. ***Владеть (или Иметь опыт деятельности):*** - навыками анализа защищённости информационных систем и средств обеспечения информационной безопасности; - навыками организации жизненного цикла защищённых информационных систем.
		ПК – 2.4 Разрабатывает организационно-распорядительные документы, регламентирующие порядок эксплуатации защищённых информационных системах	***Знать:*** - структуру и функционал защищённых информационных систем; -требования стандартов информационной безопасности, предъявляемые к информационным системам в защищённом исполнении и средствам обеспечения информационной безопасности. ***Уметь:*** - организовывать эксплуатацию защищённых информационных систем и средств обеспечения информационной безопасности. ***Владеть (или Иметь опыт деятельности):*** - навыками организации жизненного цикла защищённых информационных систем и средств обеспечения информационной безопасности.
ПК – 7	Способен обеспечивать документальное сопровождения процесса обеспечения информационной безопасности	ПК – 7.1 Определяет перечень объектов информатизации и информации (сведений) ограниченного доступа, подлежащих защите в организации	**Знать** -определение угрозы защищённой ИС; -классификацию и общий анализ угроз; -отличие случайных и преднамеренных угроз; **Уметь:** - проводить анализ возможных угроз и каналов утечки информации; **Владеть (или Иметь опыт дея-**

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*		
			тельности): - навыками определения угроз для защищаемой ИС;
		ПК – 7.2 Разрабатывает обоснование необходимости создания системы защиты информации в организации	**Знать:** - классификацию угроз и критерии оценки каждого вида; - виды уязвимостей в ИС. **Уметь:** - формировать критерии каждого вида угрозы в защищаемой системе; - найти потенциальные уязвимости в ИС. **Владеть (или Иметь опыт деятельности):** - навыками определения потенциальных угроз;
		ПК – 7.3 Разрабатывает эксплуатационную и техническую документацию на объект информатизации и средства защиты информации	**Знать:** - классификацию угроз информационной безопасности; - методики формирования модели угроз для информационной системы; - качественные и количественные методики оценки риска ИБ. **Уметь:** - выделять и ранжировать угрозы информационной безопасности; -определять наиболее подходящую методику для определения угрозы ИБ исходя из существующих и оригинальных методик; **Владеть (или Иметь опыт деятельности):** - навыками формирования списка угроз, актуальных для конкретной Информационной системы - навыками правильного применения выбранной методики.
ПК – 9	Способен контролировать защищённость информационных систем	ПК – 9.1 Разрабатывает методику оценки уровня защищённости информационной	***Знать:*** - исходные данные в БД предполагаемой информационной системе; - требования к уровню защищённости информационной безопасности; - комплексные показатели оценки

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*		
		системы	состояния ИС их интерпретацию; ***Уметь:*** - подготовить исходные данные в БД - проводить контроль реализации требований; - рассчитывать комплексные показатели оценки состояния ИС и их интерпретировать; - разрабатывать рекомендации на базе оценки уровня защищённости информационной системы; ***Владеть (или Иметь опыт деятельности):*** - навыками оценки данных БД; - навыками расчета комплексных показателей; - навыками разработки рекомендаций.
		ПК – 9.2 Проводит оценку соответствия уровня защищённости требованиям политики безопасности и нормативным документам	***Знать:*** - характеристики систем стандартизации в области защиты информации; - оценочные стандарты и технические спецификации: «Оранжевая книга», российские и международные стандарты оценки уровня защищённости; - виды тестирования систем информационной безопасности; ***Уметь:*** - составить перечень понятий и определений, используемых в стандартах и спецификациях; - протестировать систему защиты с целью проверки эффективности используемых в ней механизмов защиты, их устойчивости к атакам, а также с целью поиска уязвимостей. ***Владеть (или Иметь опыт деятельности):*** - навыками составления перечня понятий и определений, используемых в стандартах и спецификациях; - навыками тестирования системы

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*		
			защиты с целью проверки эффективности.
		ПК – 9.3 Разрабатывает систему мероприятий по оценке уровня защищённости информационной системы	***Знать:*** -требования по защите данных; - методы инструментального мониторинга защищенности информации; - способы и средства выявления каналов утечки информации. ***Уметь:*** - разрабатывать технический проект в части защиты информации; - проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации; - разрабатывать эксплуатационную документацию и средства защиты информации, а также организационно- распорядительные документы. ***Владеть (или Иметь опыт деятельности):*** -навыками управления проектом; -навыками оценки на основе инструментального мониторинга защищенности информации; - навыками оформления необходимой документации.
		ПК – 9.4 Определяет уязвимости защищённости телекоммуникационных систем и сетей	***Знать:*** - определение уязвимости информационных объектов и их классификацию; - понятие риска. Способы оценки рисков; - модель нарушителя информационной безопасности телекоммуникационных систем и сетей. ***Уметь:*** - выявлять потенциальные уязвимости защищённости телекоммуникационных систем; - проводить оценку рисков;

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*		
			- определять потенциальных нарушителей информационной безопасности телекоммуникационных систем и сетей. ***Владеть (или Иметь опыт деятельности):*** - навыками определения уязвимости защищённости телекоммуникационных систем и сетей; - навыками проведения оценки рисков; - навыками определения потенциальных нарушителей.
ПК – 10	Способен оценивать эффективность механизмов безопасности в информационных системах	ПК – 10.1 Оценивает эффективности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик	***Знать:*** принципы действия основных технических средств, обеспечивающих негласный съем конфиденциальной информации ***Уметь:*** осуществлять успешную классификацию угроз и объектов защиты ***Владеть (или Иметь опыт деятельности):*** навыком анализа информационной инфраструктуры объекта защиты и ее безопасности
		ПК – 10.2 Оценивает соответствие механизмов безопасности системы требованиям нормативных документов и рискам	**Знать:** нормативные документы, имеющие непосредственное отношение к обеспечению безопасности **Уметь:** применять ТСО в соответствии с их назначением **Владеть (или Иметь опыт деятельности):** навыком работы с рекомендациями и стандартами в области обеспечения ИБ объекта
		ПК – 10.3 Формулирует критерии оценки эффективности механизмов безопасности, ис-	**Знать:** этапы проектирования систем информационной безопасности с использованием ТСО; **Уметь:** нейтрализовать угрозы при помощи конкретных технических средств охраны

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*		
		пользуемых в информационных системах	**Владеть (или Иметь опыт деятельности):** навыками разработчика и администратора технических средств охраны;
		ПК – 10.4 Формулирует предложения по повышению эффективности механизмов безопасности, используемых в информационных системах	***Знать:*** критерии и методы оценивания механизмов защиты. **Уметь:** проводить анализ и оценивание механизмов защиты **Владеть (или Иметь опыт деятельности):** навыком работы по повышению эффективности задействованных комплексов безопасности

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 проектно-технологическая практика входит в часть, формируемую участниками образовательных отношений, блока 2 «Практика» основной профессиональной образовательной программы – программы магистратуры 10.04.01 Информационная безопасность профиль «Защищённые информационные системы». Практика проходит на 2 курсе в 4 семестре.

Объем производственной проектно-технологической практики, установленный учебным планом, – 3 зачетные единицы, продолжительность – 2 недели (108 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 12 часов, работа обучающегося в иных формах – 96 часов.

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

Таблица 4 – Этапы и содержание практики

№ 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 университета; 4) информация о требованиях к отчетным документам по практике; 5) первичный инструктаж по технике безопасности.	2
2	Основной этап	Работа обучающихся в профильной организации	50
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.	2
		Знакомство с содержанием деятельности профильной организации по обеспечению информационной безопасности и проводимыми в нем мероприятиями.	2
		Изучение нормативных правовых актов профильной организации по обеспечению информационной безопасности (экологическая стратегия и политика профильной организации, положения, приказы, инструкции, должностные обязанности, памятки и др.).	4
2.2	Практическая подготовка обучающихся *(непосредственное выполнение обучающимися видов работ, связанных с будущей профессиональной*	Самостоятельное проведение мониторинга и (или) производственного контроля воздействия предприятия на человека и среду обитания, в том числе измерений концентраций загрязняющих веществ в воздушной и водной среде, оценка опасности отходов, исследова-	30

	деятельностью)	ние уровня физического воздействия с помощью измерительных приборов. *Организация работы 2-3 человек и руководство их работой в процессе проведения мониторинга (или каких-либо измерений).*	
		Самостоятельная обработка и систематизация полученных данных с помощью профессиональных программных комплексов и информационных технологий. *Организация работы 2-3 человек и руководство их работой в процессе обработки и систематизации полученных данных.* Представление результатов мониторинга руководителю практики от организации	
		Самостоятельное проведение анализа результатов проведенного мониторинга. *Организация работы 2-3 человек и руководство их работой в процессе проведения анализа результатов мониторинга.* Оценка потенциальной опасности предприятия для человека и окружающей среды в сравнении с данными научных источников. Представление результатов анализа и обоснование оценки руководителю практики от организации.	
		Самостоятельная подготовка рекомендаций по повышению уровня безопасности предприятия. *Организация работы 2-3 человек и руководство их работой в процессе подготовки рекомендаций по повышению уровня безопасности предприятия.* Представление своих рекомендаций руководителю практики от организации.	
		Самостоятельное составление краткосрочного и долгосрочного прогноза развития ситуации. *Организация работы 2-3 человек и руководство их работой в процессе составления краткосрочного и долгосрочного прогнозов.* Представление своего прогноза с обоснованием руководителю практики от организации.	

3	Заключительный этап	Оформление дневника практики.	16
		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 проектно-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 проектно-технологической практике:

1) Титульный лист.
2) Содержание.
3) Введение. Цель и задачи практики. Общие сведения о предприятии, на котором проходила практика.
4) Основная часть отчета.

– Характеристика деятельности предприятия по обеспечению информационной безопасности и проводимых в нем мероприятий.

– Основные нормативные правовые акты предприятия по обеспечению информационной безопасности.

– Анализ результатов мониторинга.

– 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
ПК – 1 Способен формировать проектные решения по созданию и модернизации защищённых информационных систем	Технологии распределенных реестров Безопасность распределённых систем		Методы и средства защиты информации в системах электронного документооборота Управление разработкой систем безопасности Теоретические основы компьютерной безопасности

ПК – 2 Способен организовать работы по выполнению требований защиты информации ограниченного доступа в защищённых информационных системах		Производственная проектно-технологическая практика Подготовка к процедуре защиты и защита выпускной квалификационной работы
ПК – 7 Способен обеспечивать документальное сопровождения процесса обеспечения информационной безопасности	Организация работ по обеспечению безопасности в информационных системах	Производственная проектно-технологическая практика Подготовка к процедуре защиты и защита выпускной квалификационной работы
ПК – 9 Способен контролировать защищённость информационных систем	Оценка защищённости информационных систем Методы и средства защиты информации в системах электронного документооборота Производственная проектно-технологическая практика Подготовка к процедуре защиты и защита выпускной квалификационной работы	
ПК – 10 Способен оценивать эффективность механизмов безопасности в информационных системах	Технологии обеспечения информационной безопасности объектов Информационно-аналитические системы безопасности Экспертные системы комплексной оценки безопасности информационных и телекоммуникационных систем Производственная проектно-технологическая практика Подготовка к процедуре защиты и защита выпускной квалификационной работы	

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

Код компетенции/ этап	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
ПК – 1 завершающий	ПК – 1.1 Разрабатывает проектные документы на средства защиты	**Знать:** - нормативная база, Регламентирую-	**Знать:** средства защиты информации;	**Знать:** Нормативную базу, регламенти-

Код компетенции/ этап	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
	информации создаваемых телекоммуникационных систем и сетей ПК – 1.2 Готовит техническую и проектную документацию по вопросам создания защищённых информационных систем ПК – 1.3 Сопоставляет характеристики проектируемых решений с требованиями защиты информации ПК – 1.4 Формирует конфигурацию и состав защищённых информационных систем	щая создание средств защиты информации создаваемых телекоммуникационных систем и сетей; - источники и классификация угроз; **Уметь:** - разрабатывать проекты технических заданий на проектирование средств защиты информации; - классифицировать и оценивать угрозы ИБ для объекта информатизации; - составлять проектную документацию на систему защиты информации. **Владеть (**или **Иметь опыт деятельности):** Навыками разработки технических заданий	- источники и классификация угроз; - методы проектирования средств защиты информации создаваемых телекоммуникационных систем и сетей. **Уметь:** - разрабатывать проекты нормативно-распорядительных документов; - классифицировать и оценивать угрозы ИБ для объекта информатизации; - составлять проектную документацию на систему защиты информации. **Владеть (**или **Иметь опыт деятельности):** - навыками разработки технических заданий; - навыками разработки проектов нормативно-распорядительных документов;	рующую создание средств защиты информации создаваемых телекоммуникационных систем и сетей; - назначение и классификация средств защиты информации; - источники и классификация угроз; - методы проектирования средств защиты информации создаваемых телекоммуникационных систем и сетей. **Уметь:** - разрабатывать проекты технических заданий на проектирование средств защиты информации; - разрабатывать проекты нормативно-распорядительные документов; - классифицировать и оценивать угрозы ИБ для Объекта информатизации; - составлять проектную докумен-

Код компетенции/ этап	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
				тацию на систему защиты информации. **Владеть (**или **Иметь опыт деятельности):** - навыками разработки технических заданий; - навыками разработки проектов нормативно-распорядительных документов; - навыками оценки угроз ИБ.
ПК – 2 завершающий	ПК – 2.1 Управляет работой специалистов по созданию и эксплуатации средств защиты информации в защищённых информационных системах ПК – 2.2 Формирует комплекс мер (принципов, правил, процедур, практических приемов, методов, средств) для защиты в защищённых информационных системах ПК – 2.3 Управляет процессом разработки моделей угроз и моделей нарушителя безопасности информационных систем ПК – 2.4 Разрабатывает организа-	**Знать:** - основные методы организационного обеспечения процесса подготовки документов, регламентирующих создание защищённых информационных систем; ***Уметь:*** - готовить проектную и техническую документацию по вопросам создания защищённых информационных систем; **Владеть (или Иметь опыт деятельности):** - навыками организации проекта;	**Знать:** - организационные меры по защите информации; - нормативные правовые акты в области защиты информации. **Уметь:** - готовить проекты методических документов; - применять необходимые нормативные правовые акты; **Владеть (или Иметь опыт деятельности):** - навыками организации проекта; - навыками подготовки	**Знать:** - организационные меры по защите информации; - нормативные правовые акты в области защиты информации. **Уметь:** - готовить проектную и техническую документацию по вопросам создания защищённых информационных систем; - готовить проекты методических документов; - применять необходимые нормативные правовые акты;

Код компетенции/ этап	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
	ционно-распорядительные документы, регламентирующие порядок эксплуатации защищённых информационных системах		необходимой технической и проектной документации;	**Владеть (или Иметь опыт деятельности):** - навыками организации проекта; - навыками подготовки необходимой технической и проектной документации;
ПК – 7 завершающий	ПК – 7.1 Определяет перечень объектов информатизации и информации (сведений) ограниченного доступа, подлежащих защите в организации ПК – 7.2 Разрабатывает обоснование необходимости создания системы защиты информации в организации ПК – 7.3 Разрабатывает эксплуатационную и техническую документацию на объект информатизации и средства защиты информации	**Знать** -определение угрозы защищённой ИС; -классификацию и общий анализ угроз; -отличие случайных и преднамеренных угроз; **Уметь:** - проводить анализ возможных угроз и каналов утечки информации; **Владеть (или Иметь опыт деятельности):** - навыками определения угроз для защищаемой ИС;	**Знать:** - классификацию угроз и критерии оценки каждого вида; - виды уязвимостей в ИС. **Уметь:** - формировать критерии каждого вида угрозы в защищаемой системе; - найти потенциальные уязвимости в ИС. **Владеть (или Иметь опыт деятельности):** - навыками определения потенциальных угроз;	**Знать:** - классификацию угроз информационной безопасности; - методики формирования модели угроз для информационной системы; - качественные и количественные методики оценки риска ИБ. **Уметь:** - выделять и ранжировать угрозы информационной безопасности; -определять наиболее подходящую методику для определения угрозы ИБ исходя из существующих и оригинальных методик; **Владеть (или Иметь опыт деятельности):**

Код компетенции/ этап	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
				- навыками формирования списка угроз, актуальных для конкретной информационной системы - навыками правильного применения выбранной методики.
ПК – 9 завершающий	ПК – 9.1 Разрабатывает методику оценки уровня защищённости информационной системы ПК – 9.2 Проводит оценку соответствия уровня защищённости требованиям политики безопасности и нормативным документам ПК – 9.3 Разрабатывает систему мероприятий по оценке уровня защищённости информационной системы ПК – 9.4 Определяет уязвимости защищённости телекоммуникационных систем и сетей	***Знать:*** - исходные данные в БД предполагаемой информационной системе; - комплексные показатели оценки состояния ИС их интерпретацию; ***Уметь:*** - проводить контроль реализации требований; - рассчитывать комплексные показатели оценки состояния ИС и их интерпретировать; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками оценки данных БД; - навыками разработки рекомендаций.	***Знать:*** - требования к уровню защищённости информационной безопасности; - комплексные показатели оценки состояния ИС их интерпретацию; ***Уметь:*** - подготовить исходные данные в БД - проводить контроль реализации требований; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками оценки данных БД; - навыками расчета комплексных показателей; - навыками разработки рекомендаций	***Знать:*** - характеристики систем стандартизации в области защиты информации; - оценочные стандарты и технические спецификации: «Оранжевая книга», российские и международные стандарты оценки уровня защищённости; - виды тестирования систем информационной безопасности; ***Уметь:*** - составить перечень понятий и определений, используемых в стандартах и спецификациях; - протестировать систему защиты с целью проверки эффективности используемых в

Код компетенции/ этап	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
				ней механизмов защиты, их устойчивости к атакам, а также с целью поиска уязвимостей. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками составления перечня понятий и определений, используемых в стандартах и спецификациях; - навыками тестирования системы защиты с целью проверки эффективности.
ПК – 10 завершающий	ПК – 10.1 Оценивает эффективности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик ПК – 10.2 Оценивает соответствие механизмов безопасности системы требованиям нормативных документов и рискам ПК – 10.3 Формулирует критерии оценки эффективности механизмов безопас-	**Знать:** - определение уязвимости информационных объектов и их классификацию; - понятие риска. Способы оценки рисков; **Уметь:** - выявлять потенциальные уязвимости защищённости телекоммуникационных систем; - проводить оценку рисков; **Владеть (или Иметь опыт деятельности):**	**Знать:** - понятие риска. Способы оценки рисков; **Уметь:** - проводить оценку рисков; - определять потенциальных нарушителей информационной безопасности телекоммуникационных систем и сетей. **Владеть (или Иметь опыт деятельности):** - навыками определения уязвимости	***Знать:*** - модель нарушителя информационной безопасности телекоммуникационных систем и сетей. ***Уметь:*** - выявлять потенциальные уязвимости защищённости телекоммуникационных систем; - определять потенциальных нарушителей информационной безопасности

Код компетенции/ этап	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
	ности, используемых в информационных системах ПК – 10.4 Формулирует предложения по повышению эффективности механизмов безопасности, используемых в информационных системах	- навыками определения уязвимости защищённости телекоммуникационных систем и сетей; - навыками проведения оценки рисков;	защищённости телекоммуникационных систем и сетей; - навыками проведения оценки рисков; - навыками определения потенциальных нарушителей.	телекоммуникационных систем и сетей. **Владеть (или Иметь опыт деятельности):** - навыками определения уязвимости защищённости телекоммуникационных систем и сетей; - навыками проведения оценки рисков; - навыками определения потенциальных нарушителей.

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	Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности
ПК-1	Отчет о практике. Ответы на вопросы по содержанию практики на промежуточной аттестации.

ПК-2	Типовое задание № 1 по практической подготовке, предусматривающее выполнение обучающимся вида(ов) работ, связанного(ых) с будущей профессиональной деятельностью (задание конкретизируется с учетом особенностей конкретной профильной организации в Дневнике практики, в п.1.4 задания студенту): *Подготовьте паспорт объекта информатизации для проведения аттестационных испытаний по защите информации.* Дневник практики. Раздел отчета о практике – *Результаты проведенного мониторинга (и (или) производственного контроля) воздействия предприятия на человека и среду обитания.*
ПК-7	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): Разработайте рекомендации по повышению уровня безопасности предприятия, основываясь на результатах проведенного мониторинга (производственного контроля). Дневник практики. Разделы отчета о практике: – Анализ результатов мониторинга.
ПК-9	Типовое задание № 3 по практической подготовке, предусматривающее выполнение обучающимся вида(ов) работ, связанного(ых) с будущей профессиональной деятельностью (задание конкретизируется с учетом особенностей конкретной профильной организации в Дневнике практики, в п.1.4 задания студенту): Результаты проведенного мониторинга (и (или) производственного контроля) работоспособности ТКС. Дневник практики. Раздел отчета о практике – Рекомендации по повышению уровня информационной безопасности предприятия.
ПК-10	Дневник практики. Отчет о практике. 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 проектно-

технологической 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 программы	1
		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)	Полнота, точность, аргументированность ответов,	4

	4 балла		

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 : учебное пособие / Ю. Ю. Громов [и др.]. - Старый Оскол : ТНТ, 2013. - 384 с. - Текст : непосредственный.

2. Нестеров, С. А. Основы информационной безопасности : учебное пособие / С. А. Нестеров. - Санкт-Петербург : Издательство Политехнического университета, 2014. - 322 с. : табл., ил. - URL: http://biblioclub.ru/index.php?page=book&id=363040 (дата обращения: 03.03.2022) . - Режим доступа: по подписке. - Текст : электронный.

3. Степанова, Е. Е. Информационное обеспечение управленческой деятельности : учебное пособие / Е. Е. Степанова, Н. В. Хмелевская. - М. : Форум, 2004. - 154 с. - (Профессиональное образование). - Текст : непосредственный.

Дополнительная литература:

4. Аверченков, В. И. Аудит информационной безопасности : учебное пособие для вузов / В. И. Аверченков. - 4-е изд., стереотип. - Москва : Флинта, 2021. - 269 с. - URL: http://biblioclub.ru/index.php?page=book&id=93245 (дата обращения: 03.03.2022) . - Режим доступа: по подписке. - Текст : электронный.

5. Абрамов, Г. В. Проектирование информационных систем : учебное пособие / Г. В. Абрамов, И. Е. Медведкова, Л. А. Коробова. - Воронеж : Во-

ронежский государственный университет инженерных технологий, 2012. - 172 с. - URL: http://biblioclub.ru/index.php?page=book&id=141626 (дата обращения: 03.03.2022) . - Режим доступа: по подписке. - Текст : электронный.

6. Древс, Ю. Г. Организация ЭВМ и вычислительных систем : учебник / Ю. Г. Древс. - М. : Высшая школа, 2006. - 501 с. : ил. - Текст : непосредственный.

7. Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю. Н. Загинайлов. - Москва ; Берлин : Директ-Медиа, 2015. - 253 с. - URL: http://biblioclub.ru/index.php?page=book&id=276557 (дата обращения: 03.03.2022) . - Режим доступа: по подписке. - Текст : электронный.

8. Лопин, В. Н. Защита информации в компьютерных системах : 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. : ил. - Текст : непосредственный.

9. Олифер, В. Г. Сетевые операционные системы : учебное пособие / В. Г. Олифер, Н. А. Олифер. - СПб. : Питер, 2003. - 539 с. - Текст : непосредственный.

10. Петренко, В .И. Теоретические основы защиты информации : учебное пособие / В. И. Петренко. - Ставрополь : СКФУ, 2015. - 222 с. - URL: http://biblioclub.ru/index.php?page=book&id=458204 (дата обращения: 03.03.2022) . - Режим доступа: по подписке. - Текст : электронный.

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 Электронно-библиотечная система «Университетская библиотека Онлайн» – http://biblioclub.ru

2 Электронная библиотека диссертаций и авторефератов РГБ – http://dvs.rsl.ru

3 Базы данных ВИНИТИ РАН – http://viniti.ru

9 Описание материально-технической базы, необходимой для проведения практики

Для проведения практики используется технологическое и метрологическое оборудование конкретной профильной организации, на базе которой она проводится:

– современная измерительная техника: устройства, позволяющие осуществлять контроль параметров окружающей среды, 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 – 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 вы-

соту 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
	измененных	замененных	аннулированных	новых			