МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:
И.о. декана факультета ФиПИ
_____ Таныгин М.О.
(подпись, инициалы, фамилия)
«30» 08 2021 г.

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

Производственная эксплуатационная практика
(наименование вида и типа практики)

ОПОП ВО 10.03.01 Информационная безопасность
шифр и наименование направление подготовки (специальности)

Безопасность автоматизированных систем в сфере информационных и
наименование направленности (профиля, специализации)
коммуникационных технологий

форма обучения *очная*
очная, очно-заочная, заочная

Курск – 2021

Рабочая программа практики составлена в соответствии с:

– федеральным государственным образовательным стандартом высше-го образования – бакалавриат по направлению подготовки 10.03.01 «Инфор-мационная безопасность», утвержденным приказом Минобрнауки России от 17 ноября 2020 г. №1427;

– ОПОП ВО 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий», 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 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий» на заседании кафедры информационной безопасности «30» августа 2021 г., протокол № 1.

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 10.03.01 Информационная безопасность на основании учебного плана ОПОП ВО 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий», одобренного Ученым советом университета протокол №6 «26» 02 20 21 г., на заседании кафедры ИБ №11. от 30.06.2022г.

(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 10.03.01 Информационная безопасность на основании учебного плана ОПОП ВО 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий», одобренного Ученым советом университета протокол №__«___» _____ 20 ___ г., на заседании кафедры_____.

(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 10.03.01 Информационная безопасность на основании учебного плана ОПОП ВО 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)», одобренного Ученым советом университета протокол №__«___» _______ 20 ___ г., на заседании кафедры______________________.
(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 10.03.01 Информационная безопасность на основании учебного плана ОПОП ВО 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)», одобренного Ученым советом университета протокол №__«___» _______ 20 ___ г., на заседании кафедры______________________.
(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 10.03.01 Информационная безопасность на основании учебного плана ОПОП ВО 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)», одобренного Ученым советом университета протокол №__«___» _______ 20 ___ г., на заседании кафедры______________________.
(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 10.03.01 Информационная безопасность на основании учебного плана ОПОП ВО 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)», 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 преддипломной практики является получение профессиональных умений и опыта профессиональной деятельности в области проектирования и реализации технологий информационной безопасности.

1.2. Задачи практики

1. Формирование общепрофессиональных компетенций, установленных ФГОС ВО и закрепленных учебным планом за производственной эксплуатационной 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 – эксплуатационная.

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 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	*наименование*		
ОПК-1	Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;	ОПК-1.1 Классифицирует угрозы информационной безопасности в соответствии с нормативными документами	***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 информационных систем.
		ОПК-1.2 Оценивает угрозы информационной безопасности с точки зрения основных концепций национальной безопасности Российской Федерации	***Знать:*** - концепцию национальной безопасности РФ; - технологии повышения защищенности распределенных информационных систем; - административную, уголовную, гражданско-правовую ответственность. ***Уметь:*** - выполнять определять характер угрозы и масштабы последствий; - минимизировать последствия ущерба за счет интеграции средств защиты. ***Владеть (или Иметь опыт деятельности):*** - навыками оценки угроз ИБ с точки зрения нормативно-правового обеспечения; - навыками ранжирования угроз с учетом масштаба возможных последствий;
		ОПК-1.3 Определяет	***Знать:***

		угрозы информационной безопасности для различных систем	- методы повышения уровня защищенности информационных систем; - стандарты, предназначенные для контроля качества процессов защиты исследуемого объекта - нормативно-правовые аспекты обеспечения информационной безопасности. ***Уметь:*** - формализовать сведения для запросов; - выбирать тип запроса; - составлять простые и составные запросы. ***Владеть (****или* ***Иметь опыт деятельности):*** - общими приемами организации поиска; - алгоритмическими схемами стратегий поиска; - навыками программирования поисковых процедур.
ОПК -5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;	ОПК-5.1 Разрабатывает проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации	***Знать:*** - правовые основы организации защиты конфиденциальной информации; - задачи органов защиты информации; ***Уметь:*** - применять действующую законодательную базу в области обеспечения информационной безопасности; - классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; - разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками работы с нормативными правовыми актами; - навыками разработки проектов локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации.
		ОПК-5.2 Формулирует основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации	***Знать:*** - правовые нормы и стандарты по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации; - принципы формирования политики информационной безопасности в автоматизированных системах. ***Уметь:*** - применять действующую законодательную базу по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации; - разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организа-

			ции. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками работы с нормативными правовыми актами; - навыками разработки проектов локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации.
		ОПК-5.3 Формулирует основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации	***Знать:*** **-** правовые нормы и стандарты по лицензированию в области обеспечения защиты информации и сертификации средств защиты; - основные отечественные и зарубежные стандарты в области информационной безопасности; - терминологию, основные руководящие и регламентирующие документы в области ЭВМ, комплексов и систем. ***Уметь:*** **-** применять действующую законодательную базу в области обеспечения информационной безопасности при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации; - разрабатывать проекты локальных правовых актов, инструкций, регламентов при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками работы с нормативными правовыми актами; - навыками работы с технической документацией на ЭВМ и вычислительные системы; - навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках.
ОПК-6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	ОПК-6.2 Определяет политику контроля доступа работников к информации ограниченного доступа	***Знать:*** **-** основные требования, предъявляемые к сотрудникам защиты информации ограниченного доступа; - угрозы безопасности; - модели нарушителя объекта информатизации. ***Уметь:*** - составлять перечень лиц, имеющих доступ к информации ограниченного доступа; - разрабатывать требования, предъявляемые к контролю доступа сотрудников к информации ограниченного доступа***;*** ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками формулирования основных требований, предъявляемых к организации защиты информации ограниченного доступа; - навыками создания локальных нормативных актов.
ОПК-9	Способен применять средства криптогра-	ОПК-9.3 Организует защиту информации от	***Знать:*** - основные виды угроз безопасности

	фической и технической защиты информации для решения задач профессиональной деятельности;	утечки по техническим каналам на объектах информатизации	- возможные каналы утечки конфиденциальной информации по техническим каналам; - принципы организации защиты информации от утечки по техническим каналам. ***Уметь:*** **-** выполнять требования нормативных и эксплуатационных документов (документации) по обеспечению защиты информации, - определять каналы утечки информации; - организовывать мероприятия, направленные на защиту информации. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками применения технических средств защиты информации. - навыками определения каналов утечки; - навыками планирования, контроля.
		ОПК-9.5 Использует средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации	***Знать:*** - нормативные документы; -средства защиты информации от утечки по техническим каналам; - средства контроля эффективности защиты информации; ***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 (****или* ***Иметь опыт деятельности):*** **-** навыками эксплуатации средств защиты информации и анализа защищенности телекоммуникационных систем и сетей; - методами проведения анализа угроз информационной безопасности.
ОПК-10	Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;	ОПК-10.1 Реализует требования политик безопасности на объектах информатизации	***Знать:*** - требования политик безопасности на объектах информатизации; - систему хранения и обработки информации; - принципы идентификации записей. ***Уметь:*** - применять требования политик безопасности на объектах информатизации; - организовывать выполнение мер по обеспечению информационной безопасности. ***Владеть (****или* ***Иметь опыт деятельности):*** **-** навыками управления; - навыками создания локально-нормативных документов.
		ОПК-10.2 Конфигурирует программно-аппаратные средства защиты информации в соответствии с заданными политиками без-	***Знать:*** - основные угрозы компьютерной информации, реализуемые на различных уровнях программной иерархии и типы атак; - основные принципы построения подсистем защиты компьютерной информации в операционных системах и в

		опасности	пользовательских программных приложениях; - сертифицированные и перспективные программно-аппаратные средства и методы защиты компьютерной информации; - принципы функционирования основных типов вредоносных программ, способы их выявления и нейтрализации. ***Уметь:*** - выявлять слабости защиты ОС, ВС и СУБД и использовать их для вскрытия защиты; - планировать программно-аппаратную подсистему политики безопасности организации; - применять и администрировать средства программно-аппаратной защиты информации. - производить анализ эффективности программно-аппаратных средств защиты информации в компьютерных сетях; - оценивать оптимальность выбора программно-аппаратных средств. ***Владеть (****или* ***Иметь опыт деятельности):*** - методами администрирования операционных систем и баз данных; - методами защиты информации в операционных системах и в пользовательских приложениях; - способами выявления основных вредоносных программ и их нейтрализацией; - навыками анализа и администрирования подсистем защиты современных ОС, ВС и СУБД; - навыками использования межсетевых экранов и систем обнаружения вторжений.
		ОПК-10.3 Применяет средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях	***Знать:*** - принципы построения компьютерных сетей, операционных систем; - стек сетевых протоколов операционных систем, стек протоколов сетевого оборудования; - порядок реализации методов и средств межсетевого экранирования; - принципы функционирования сетевых протоколов, включающих криптографические алгоритмы; - методы измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации - принципы работы и правила эксплуатации эксплуатируемых программно-аппаратных средств защиты информации - нормативные правовые акты в области защиты информации; ***Уметь:*** - оценивать угрозы безопасности информации в компьютерных сетях, операционных системах, БД; - обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных сетях; - выбирать режимы работы программно-аппаратных средств защиты

			информации в компьютерных сетях, ОС; - проводить мониторинг функционирования программно-аппаратных средств защиты информации в компьютерных сетях, операционных системах; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками определения состава применяемых программно-аппаратных средств защиты информации в компьютерных сетях; - навыками разработки порядка применения программно-аппаратных средств защиты информации в компьютерных сетях; - навыками настройки программных и аппаратных средств построения компьютерных сетей, использующих криптографическую защиту информации
ОПК-12	Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;	ОПК-12.4 Разрабатывает основные показатели технико-экономического обоснования соответствующих проектных решений	***Знать:*** - основные методы управления информационной безопасностью; - основные понятия теории автоматов, математической логики, теории алгоритмов и теории графов; - основные отечественные и зарубежные стандарты в области защиты информации; -основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические) - угрозы безопасности, информационные воздействия, критерии оценки защищенности и методы защиты информации в автоматизированных системах; ***Уметь:*** **-** проводить технико-экономическое обоснование проектных решений программно-аппаратных средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня защищенности - исследовать эффективность проектных решений программно-аппаратных средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня защищенности; -проводить комплексное тестирование и отладку аппаратных и программных систем защиты информации ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками управления информационной безопасности; - навыками подготовки исходных данных для проектирования подсистем; - навыками оценки эффективности проектных решений;
ОПК -4.1	Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах	ОПК-4.1.4 Готовит документы, определяющие правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной систе-	***Знать:*** - нормативно-правовую базу стандартизации работы оператора при обеспечении защиты информации; - стандарты в области системной и программной инженерии; - стандарты на техническую документацию и процессы документирования.

		ме в ходе ее эксплуатации	***Уметь:*** **-** формулировать требования к оператору для обеспечения защиты информации; - описывать бизнес-процессы и требования к порядку их выполнения; - подготавливать необходимые документы, регламентирующие действия оператора при эксплуатации информационной системы с целью защиты информации. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками формулировки требований; - навыками описания бизнес-процессов; -навыками разработки документов.
ОПК-4.3	Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем	ОПК-4.3.1 Осуществляет автономную наладку технических и программных средств системы защиты информации автоматизированной системы	***Знать:*** - принципы автономной наладки технических и программных средств системы защиты информации автоматизированной системы; - порядок эксплуатации средств антивирусной защиты; - порядок обеспечения безопасности при эксплуатации технических и программных средств; ***Уметь:*** **-** устанавливать программные и технические средства в соответствии с технической документацией; -производить настройку параметров работы технических и программных средств ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками установки антивирусной защиты; - навыками настройки встроенных средств защиты информации программного обеспечения.
		ОПК-4.3.2 Применяет типовые программные средства резервирования и восстановления информации в автоматизированных системах	***Знать:*** - перечень информации, подлежащей резервному копированию; - методику проведения резервного копирования; - принципы восстановления информации в автоматизированных системах. ***Уметь:*** **-** применять типовые программные средства резервирования и восстановления информации в автоматизированных системах; - настраивать систему резервного копирования; - проверять корректность резервной копии. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками фильтрации информации, подлежащей резервному копированию; - навыками применения методик резервного копирования и восстановления.
		ОПК-4.3.3 Устраняет известные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации	***Знать:*** - общие принципы функционирования вредоносного программного обеспечения; - сущность источников угроз информационной безопасности, связанных с эксплуатацией автоматизированной системы; - типовые уязвимости автоматизированной системы и методы их эксплуатации ***Уметь:***

			- обнаружить уязвимости автоматизированной системы; - устранить уязвимости автоматизированной системы; - разработать рекомендации по предотвращению повторения уязвимости. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками определения уязвимости автоматизированных систем; - навыками разработки документации.

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 эксплуатационная практика входит в обязательную часть блока 2 «Практика» основной профессиональной образовательной программы – программы специалитета 10.03.02 Информационная безопасность, профиль «Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)». Практика проходит на 6 курсе в 11 семестре.

Объем производственной эксплуатационной практики, установленный учебным планом, – 3 зачетные единиц, 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 (часы указаны в учебном плане в графе «Пр»), работа обучающегося в иных формах – 96 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	Решение организационных вопросов:	2

	этап	1) распределение обучающихся по местам практики; 2) знакомство с целью, задачами, программой, порядком прохождения практики; 3) получение заданий от руководителя практики от университета; 4) информация о требованиях к отчетным документам по практике; 5) первичный инструктаж по технике безопасности.	
2	Основной этап	Работа обучающихся в профильной организации	80
2.1	Знакомство с профильной организацией	Знакомство с профильной организацией, руководителем практики от организации, рабочим местом и должностной инструкцией.	3
		Инструктаж по технике безопасности на рабочем месте.	3
		Знакомство с содержанием деятельности профильной организации по обеспечению информационной безопасности и проводимыми в нем мероприятиями.	
		Изучение нормативных правовых актов профильной организации по обеспечению информационной безопасности (политика безопасности профильной организации, положения, приказы, инструкции, должностные обязанности, памятки и др.).	2
2.2	Практическая подготовка обучающихся *(непосредственное выполнение обучающимися видов работ, связанных с будущей профессиональной деятельностью)*	Самостоятельное проведение мониторинга и (или) производственного контроля эксплуатации средств защиты информации в ТКС. Организация работы 2-3 человек и руководство их работой в процессе проведения мониторинга безопасности ТКС. Создание плана работы коллектива из 3 – 4 человек, реализующего политику безопасности в ТКС	72

		Самостоятельная обработка и систематизация полученных данных с помощью профессиональных программных комплексов и информационных технологий. *Формирование систематизированной инструкции по эксплуатации конкретного средства защиты информации в конкретной ТКС.* Представление результатов мониторинга руководителю практики от организации	
		Самостоятельное проведение уценки угроз информационной безопасности, возможных каналов утечек конфиденциальных данных в ТКС. Оценка рисков информационной безопасности. Представление результатов анализа и обоснование оценки руководителю практики от организации.	
		Самостоятельная подготовка рекомендаций по повышению уровня информационной безопасности предприятия. *Организация работы 2-3 человек и руководство их работой в процессе подготовки рекомендаций по проведению регламентных работ по обнаружению уязвимостей ТКС.* Представление своих рекомендаций руководителю практики от организации.	
		Самостоятельное составление рекомендаций по отказоустойчивой эксплуатации защищённых ТКС. Представление перечня средств и мер по обеспечению отказоустойчивости системы.	
3	Заключительный этап	Оформление дневника практики.	26
		Составление отчета о практике.	
		Подготовка графических материалов для отчета.	
		Представление дневника практики и защита отчета о практике на промежуточной аттестации.	

5 Указание форм отчетности по практике

Формы отчетности студентов о прохождении производственной производственной практики:

– дневник практики (форма дневника практики приведена на сайте университета *https://www.swsu.ru/structura/umu/training_division/blanks.php),*

– отчет о практике.

Структура отчета о производственной преддипломной практике:

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

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

– Основные нормативные правовые акты предприятия по обеспечению информационной безопасности.

– Анализ результатов 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	Основы информационной безопасности	Производственная эксплуатационная практика Основы управления информационной безопасностью	Гуманитарные аспекты информационной безопасности
ОПК-5	Организационное и правовое обеспечение информационной безопасности	Основы управления информационной безопасностью	Производственная эксплуатационная практика
ОПК-6	Организационное и правовое обеспечение информационной безопасности	Основы управления информационной безопасностью	Производственная эксплуатационная практика
ОПК-9	Основы информационной безопасности Учебно-лабораторная практика	Методы и средства криптографической защиты информации Производственная эксплуатационная практика	Защита информации от утечки по техническим каналам Безопасность сетей ЭВМ Сети и системы передачи информации
ОПК-10	Производственная эксплуатационная практика	Безопасность сетей ЭВМ	Программно-аппаратные средства защиты информации
ОПК-12	Основы управления информационной безопасностью	Производственная эксплуатационная практика	Программно-аппаратные средства защиты информации Экономическое обоснование проектных решений
ОПК-4.1	Основы управления информационной безопасностью	Организационное и правовое обеспечение информационной безопасности	Производственная эксплуатационная практика
ОПК-4.3	Производственная эксплуатационная практика		Программно-аппаратные средства защиты информации

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/ основной	ОПК-1.1 Классифицирует угрозы информационной безопасности в соответствии с нормативными документами	***Знать:*** - основные угрозы информационной безопасности; ***Уметь:*** - выявлять угрозы информационной безопасности; - 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; ***Уметь:*** - выявлять угрозы информационной безопасности; - снижать вероятность отрицательных последствий сетевого взаимодействия; - классифицировать угрозы информационной безопасности; - ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками классификации угроз ;	***Знать:*** - 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 информационных систем.
	ОПК-1.2 Оценивает угрозы информаци-	***Знать:*** - концепцию наци-	***Знать:*** - технологии по-	***Знать:*** - концепцию наци-

1	2	3	4	5
	онной безопасности с точки зрения основных концепций национальной безопасности Российской Федерации	ональной безопасности РФ; **- административную, уголовную, гражданско-правовую ответственность.** ***Уметь:*** - минимизировать последствия ущерба за счет интеграции средств защиты. ***Владеть (или Иметь опыт деятельности):*** - навыками ранжирования угроз с учетом масштаба возможных последствий;	вышения защищенности распределенных информационных систем; ***Уметь:*** - выполнять определять характер угрозы и масштабы последствий; ***Владеть (или Иметь опыт деятельности):*** - навыками ранжирования угроз с учетом масштаба возможных последствий;	ональной безопасности РФ; - технологии повышения защищенности распределенных информационных систем; **- административную, уголовную, гражданско-правовую ответственность.** ***Уметь:*** - выполнять определять характер угрозы и масштабы последствий; - минимизировать последствия ущерба за счет интеграции средств защиты. ***Владеть (или Иметь опыт деятельности):*** - навыками оценки угроз ИБ с точки зрения нормативно-правового обеспечения; - навыками ранжирования угроз с учетом масштаба возможных последствий;
	ОПК-1.3 Определяет угрозы информационной безопасности для различных систем	***Знать:*** - основы работы в режиме пошаговой отладки передачи конфиденциальных данных в информационной системе; ***Уметь:*** - выполнять выявление контрафактной продукции; - выводить сообщения в случае возникновения не-	***Знать:*** - особенности вывода промежуточных значений в ходе работы отдельных модулей информационных систем; - основы использования средств защиты информации. ***Уметь:*** - организовать безопасную работу в Интернет;	***Знать:*** - основы работы в режиме пошаговой отладки передачи конфиденциальных данных в информационной системе; - особенности вывода промежуточных значений в ходе работы отдельных модулей информационных систем; - основы использо-

1	2	3	4	5
		штатных ситуаций работы информационной системы; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками установки программных средств защиты; - навыками оценки защищенности информационной системы с учетом возможных угроз.	- выводить сообщения в случае возникновения нештатных ситуаций работы информационной системы; - интегрировать средства защиты на программном уровне. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками установки программных средств защиты; - навыками оценки защищенности информационной системы с учетом возможных угроз.	вания средств защиты информации. ***Уметь:*** - выполнять выявление контрафактной продукции; - организовать безопасную работу в Интернет; - выводить сообщения в случае возникновения нештатных ситуаций работы информационной системы; - интегрировать средства защиты на программном уровне. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками установки программных средств защиты; - технологией ведения протокола работы системы с выводом промежуточных результатов обработки данных. - навыками оценки защищенности информационной системы с учетом возможных угроз.
ОПК–5/ завершающий	ОПК-5.1 Разрабатывает проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентиру-	Знать: -стандарты в области информационной безопасности; Уметь: - сопоставлять характеристики правового обеспечения действующим стан-	Знать: - методологические подходы применения нормативных документов при оценке защищённости правового обеспечения; Уметь:	Знать: - принципы формирования комплексных отчётов по аудиту информационной безопасности; Уметь: - вырабатывать методические

1	2	3	4	5
	ющих работу по обеспечению информационной безопасности в организации	дартам, Владеть: - комплексной оценкой защищённости систем документооборота	- выявлять не декларируемые угрозы; Владеть: - способностью к критическому анализу используемых методов аудита информационной безопасности	рекомендации по формированию политик безопасности; Владеть: - организационными формами и методами проведения научных исследований
	ОПК-5.2 Формулирует основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации	Знать: - основные нормативные правовые документы. Уметь: - ориентироваться в системе законодательства и нормативных правовых актов в области защиты информации. Владеть: - навыками поиска необходимых нормативных и законодательных документов и навыками работы с ними в профессиональной деятельности	Знать: - нормативно правовые документы. Уметь: - использовать нормативно правовые акты в задачах защиты информации Владеть: - навыками поиска необходимых нормативных и законодательных документов и навыками анализа результатов их применения.	Знать: - Российские и международные нормативно правовые документы в области защиты информации. Уметь: - разрабатывать рекомендации по применению нормативно правовых документов в области защиты информации. Владеть: - навыками разработки организационно-распорядительной документации на объекте информатизации
	ОПК-5.3 Формулирует основные требования при лицензировании	Знать: - основные нормативные правовые докумен-	Знать: - нормативно правовые документы.	Знать: - Российские и международные нормативно пра-

1	2	3	4	5
	деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации	ты. Уметь: - ориентироваться в системе законодательства и нормативных правовых актов в области защиты информации. Владеть: - навыками поиска необходимых нормативных и законодательных документов и навыками работы с ними в профессиональной деятельности	Уметь: - использовать нормативно правовые акты в задачах защиты информации Владеть: - навыками поиска необходимых нормативных и законодательных документов и навыками анализа результатов их применения.	вовые документы в области защиты информации. Уметь: - разрабатывать рекомендации по применению нормативно правовых документов в области защиты информации. Владеть: - навыками разработки организационно-распорядительной документации на объекте информатизации
ОПК-6 завершающий	ОПК-6.2 Определяет политику контроля доступа работников к информации ограниченного доступа	***Знать*** основные требования, предъявляемые к организации защиты информации ограниченного доступа ***Уметь:*** формулировать 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*** требования, предъявляемые к организации защиты информации ограниченного доступа 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*** 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 требований, предъявляемых к организации защиты информации ограниченного доступа

1	2	3	4	5
ОПК-9/ завершающий	ОПК-9.3 Организует защиту информации от утечки по техническим каналам на объектах информатизации	Знать: виды угроз и возможные каналы утечки конфиденциальной информации по техническим каналам. Уметь: выполнять требования нормативных и эксплуатационных документов (документации) по обеспечению защиты информации в телекоммуникационных системах и вскрытия каналов утечки информации, по организации мероприятий, направленных на защиту информации. Владеть: навыками разработки нормативных и технических документов по организации защиты информации в телекоммуникационных системах.	Знать: основные тактико-технические характеристики, принципы построения технических средств передачи и защиты информации, виды сигналов и способы распространения радиоволн, принципы и способы организации системы защиты информации. Уметь: разрабатывать нормативную документацию по выполнению требований защиты в телекоммуникационных системах. Владеть: навыками применения технических средств защиты информации.	Знать: порядок и алгоритм проведения организационных мероприятий на объектах информатизации. Функциональные обязанности по организации мероприятий по защите информации в телекоммуникационных системах. Уметь: осуществлять выбор технических средств защиты информации в зависимости от условий эксплуатации в телекоммуникационных систем. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями инструкций, эксплуатационной документации. Владеть: навыками проведения организационных мероприятий по вскрытию уязвимых мест систем обеспечения защиты информации телекоммуникационных систем.
	ОПК-9.5 Использует средства защиты информации от утечки по техническим каналам и	Знать: классификацию, принципы, способы и порядок функционирования средств защиты	Знать: основные угрозы, предотвращаемые, СЗИ; виды, методы и средства контроля защиты ин-	Знать: нормативные документы регламентирующие порядок проведения контроля защиты ин-

1	2	3	4	5
	контроля эффективности защиты информации	информации, принципы организации проверок технических СЗИ, инструментальные средства проведения проверок технических СЗИ. Уметь: анализировать нормативную документацию, регламентирующую порядок проведения контроля защиты информации. Владеть: навыками организации контрольных проверок технических СЗИ, эксплуатации средств защиты информации и средств контроля защиты информации в соответствии с эксплуатационной документацией.	формации. Уметь: организовать комплекс мероприятий контроля эффективности защиты информации, в соответствии регламентирующими документами. Владеть: требованиями нормативной документации, регламентирующей порядок проведения контроля защиты информации.	формации, комплекс мероприятий, проводимых в ходе контроля эффективности защиты информации. Уметь: применятьсредства защиты информации и средства контроля защиты информации в соответствии с эксплуатационной документацией. Владеть: навыками применения комплекса мероприятий контроля эффективности защиты информации.
ОПК-10/ завершающий	ОПК-10.1 Реализует требования политик безопасности на объектах информатизации	***Знать:*** отдельные этапы жизненного цикла автоматизированных систем и регламентные мероприятия на каждом из них ***Уметь:*** выполнять действия по обеспечению информационной безопасности автоматизированных систем ***Владеть (****или* ***Иметь опыт деятельности):*** систематизации отдельных действие	***Знать:*** основные этапы жизненного цикла автоматизированных систем и регламентные мероприятия на каждом из них ***Уметь:*** выполнять последовательности действий по обеспечению информационной безопасности автоматизированных систем ***Владеть (****или* ***Иметь опыт деятельности):*** си-	***Знать:*** все этапы жизненного цикла автоматизированных систем и регламентные мероприятия на каждом из них ***Уметь:*** выполнять связанные последовательности действий по обеспечению информационной безопасности автоматизированных систем ***Владеть (****или* ***Иметь опыт деятельности):*** си-

1	2	3	4	5
		по обеспечению информационной безопасности автоматизированных систем	стематизации действие по обеспечению информационной безопасности автоматизированных систем	стематизации последовательности действий по обеспечению информационной безопасности автоматизированных систем
	ОПК-10.2 Конфигурирует программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности	***Знать:*** Структуру и содержание отдельных профилей заданий по безопасности для оборудования телекоммуникационных систем в защищённом исполнении ***Уметь:*** структурировать небольшие последовательности процедур и регламентных работ в единые систематические профили безопасности ***Владеть (****или* ***Иметь опыт деятельности):*** навыками эксплуатации оборудования телекоммуникационных систем	***Знать:*** Структуру и содержание профилей заданий по безопасности для оборудования телекоммуникационных систем в защищённом исполнении ***Уметь:*** структурировать отдельные процедуры и регламентные работы в единые систематические профили безопасности ***Владеть (****или* ***Иметь опыт деятельности):*** навыками эксплуатации оборудования телекоммуникационных систем в защищённом исполнении	***Знать:*** Методику формирования профилей заданий по безопасности для оборудования телекоммуникационных систем в защищённом исполнении ***Уметь:*** структурировать сложные последовательности процедур и регламентных работ в единые систематические профили безопасности ***Владеть (****или* ***Иметь опыт деятельности):*** уверенными навыками эксплуатации оборудования телекоммуникационных систем в защищённом исполнении
	ОПК-10.3 Применяет средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях	***Знать:*** шкалы результативности применения штатных средств обеспечения информационной безопасности ***Уметь:*** использовать количественные критерии результативности применения штатных средств обеспечения информационной безопасности ***Владеть (****или*	***Знать:*** критерии результативности применения штатных средств обеспечения информационной безопасности ***Уметь:*** формулировать количественные критерии результативности применения штатных средств обеспечения информационной безопасности ***Владеть (****или*	***Знать:*** методику оценки результативности применения штатных средств обеспечения информационной безопасности ***Уметь:*** формулировать методы оценки результативности применения штатных средств обеспечения информационной безопасности ***Владеть (****или* ***Иметь опыт дея-***

1	2	3	4	5
		Иметь опыт деятельности): навыками применения штатных средств обеспечения информационной безопасности	***Иметь опыт деятельности):*** навыками оценки результативности применения штатных средств обеспечения информационной безопасности	***тельности):*** сформированными навыками оценки результативности применения различных средств обеспечения информационной безопасности
ОПК-12/ основной	ОПК-12.4 Разрабатывает основные показатели технико-экономического обоснования соответствующих проектных решений	***Знать:*** - основы экономического обоснования проекта. ***Уметь:*** - анализировать исходные данные для обоснования целесообразности разработки проекта; - применять принципы выявления ключевых параметров работы информационной системы; ***Владеть (****или* ***Иметь опыт деятельности):*** - приемами анализа полноты и корректности ключевых параметров эксплуатации;	***Знать:*** - основы формирования исходных данных для телекоммуникационных задач; ***Уметь:*** - анализировать исходные данные для обоснования целесообразности разработки проекта; - применять принципы выявления ключевых параметров работы информационной системы; ***Владеть (****или* ***Иметь опыт деятельности):*** - приемами анализа полноты и корректности ключевых параметров эксплуатации;	***Знать:*** - основы формирования исходных данных для 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 -4.1 основной	ОПК-4.1.4 Готовит документы, определяющие правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации	***Знать:*** порядок эксплуатации средств обеспечения информационной безопасности телекоммуникационных систем сетей ***Уметь:*** проводить отдельные процедуры по обеспечению информацион-	***Знать:*** порядок и правила эксплуатации средств обеспечения информационной безопасности телекоммуникационных систем сетей ***Уметь:*** проводить последовательности процедур по обеспечению ин-	***Знать:*** порядок, правила и особенности эксплуатации средств обеспечения информационной безопасности телекоммуникационных систем сетей ***Уметь:*** объединять отдельные технологии и процедуры

1	2	3	4	5
		ной безопасности в последовательности ***Владеть (или Иметь опыт деятельности):*** навыками эксплуатации некоторых средств обеспечения информационной безопасности телекоммуникационных систем сетей	формационной безопасности в последовательности ***Владеть (или Иметь опыт деятельности):*** навыками эксплуатации средств обеспечения информационной безопасности телекоммуникационных систем сетей	по обеспечению информационной безопасности в последовательности ***Владеть (или Иметь опыт деятельности):*** навыками эксплуатации разнообразных средств обеспечения информационной безопасности телекоммуникационных систем сетей
ОПК-4,3/ основной	ОПК-4.3.1 Осуществляет автономную наладку технических и программных средств системы защиты информации автоматизированной системы	***Знать:*** Профили защиты инструментальных средств обеспечения защиты информации автоматизированных систем. ***Уметь:*** настройку средств реализации профилей защиты. ***Владеть:*** Навыками наблюдения за процессом и параметров функционирования автоматизированных систем и сетей.	***Знать:*** Порядок использования профилей защиты инструментальные средства обеспечения защиты информации автоматизированных систем. ***Уметь:*** Осуществлять внедрение средств реализации профилей защиты. ***Владеть:*** Навыками описания процесса и параметров функционирования автоматизированных систем и сетей.	***Знать:*** Методику формирования профилей защиты инструментальные средства обеспечения защиты информации автоматизированных систем. ***Уметь:*** Осуществлять рациональный выбор средств реализации профилей защиты. ***Владеть:*** Навыками контроля процесса и параметров функционирования автоматизированных систем и сетей.
	ОПК-4.3.2 Применяет типовые программные средства резервирования и восстановления информации в автоматизированных системах	***Знать:*** основные каналы утечки конфиденциальной информации по техническим каналам, основные тактико-технические характеристики, принципы построения технических средств передачи и защиты информации,. ***Уметь:*** Осуществлять эксплуатацию	***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,.	***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, принци-

1	2	3	4	5
		технических средств защиты информации. ***Владеть:*** навыками фиксации инцидентов, связанных с осуществлением угроз безопасности.	***Уметь:*** Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями инструкций, эксплуатационной документации. ***Владеть:*** навыками прогнозирования рисков, связанных с осуществлением угроз безопасности.	пы и способы организации системы защиты информации на объектах информатизации. ***Уметь:*** Осуществлять эксплуатацию технических средств защиты информации в соответствии с целями политики информационной безопасности. ***Владеть:*** навыками оценки рисков, связанных с осуществлением угроз безопасности.
	ОПК-4.3.3 Устраняет известные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации	***Знать:*** номенклатуру средств защищенности телекоммуникационных систем и сетей ***Уметь:*** использовать функциональные возможности средств защиты автоматизированных систем ***Владеть*** *(или* ***Иметь опыт деятельности):*** навыками эксплуатации средств защиты автоматизированных систем в основных состояниях	***Знать:*** номенклатуру, технические характеристики средств защищенности телекоммуникационных систем и сетей ***Уметь:*** использовать функциональные возможности компонентов средств защиты автоматизированных систем для повышения защищенности систем и сетей ***Владеть*** *(или* ***Иметь опыт деятельности):*** навыками эксплуатации средств защиты автоматизированных систем в различных состояниях	***Знать:*** номенклатуру, принципы организации, технические характеристики средств защиты автоматизированных систем ***Уметь:*** использовать функциональные возможности компонентов телекоммуникационных систем и сетей для анализа защищенности систем и сетей ***Владеть*** *(или* ***Иметь опыт деятельности):*** навыками эксплуатации средств защиты автоматизированных систем состояниях

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-5 основной	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 -6 основной	Дневник практики. Отчет о практике. Ответы на вопросы по содержанию практики на промежуточной аттестации.
ОПК -9 основной	Дневник практики. Отчет о практике. Раздел отчета о практике – *Результаты работы со средствами программно-аппартной защиты информации в ТКС.* 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): *Выполнить настройку программно-аппаратного средства защиты информации в соответствие с заданной политикой информационной безопасности.* Доклад обучающегося на промежуточной аттестации (защита отчета о практике). Характеристика руководителя практики от организации управленческих качеств обучающегося.
ОПК -10 основной	Дневник практики. Отчет о практике: Доклад обучающегося на промежуточной аттестации (защита отчета о практике). Характеристика руководителя практики от организации управленческих качеств обучающегося.
ОПК -12 основной	Дневник практики. Отчет о практике. Графические материалы к отчету. Доклад обучающегося на промежуточной аттестации (защита

	отчета о практике). Характеристика руководителя практики от организации управленческих качеств обучающегося.
ОПК -4.1 завершающий	Дневник практики. 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): *Восстановите активность сетевых приложений по предложенному вам журналу брандмауэра.* Графические материалы к отчету. Раздел отчета о практике – *Результаты проведенного мониторинга (и (или) производственного контроля) работоспособности ТКС.* Отчет о практике: Доклад обучающегося на промежуточной аттестации (защита отчета о практике). Характеристика руководителя практики от организации управленческих качеств обучающегося.
ОПК -4.3.2 завершающий	Дневник практики. Отчет о практике. Типовое задание № 3 по практической подготовке, предусматривающее выполнение обучающимся вида(ов) работ, связанного(ых) с будущей профессиональной деятельностью (задание конкретизируется с учетом особенностей конкретной профильной организации в Дневнике практики, в п.1.4 задания студенту): *Реализуйте с помощью средства мониторинга сетевых соединений требуемую политику безопасности.* 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 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) 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:

1. 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.

2. 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.

3. Древс, Ю. Г. Организация ЭВМ и вычислительных систем [Текст] : учебник / Ю. Г. Древс. - М. : Высшая школа, 2006. - 501 с.

4. Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю. Н. Загинайлов. - М. ; Бер-

лин : 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.

5. 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.

6. 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.

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

8. 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.

1.ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»

2. ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»

3. Р 50.1.056-2005 «Техническая защита информации. Основные термины и определения»

4. 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»

5. ГОСТ Р ИСО/МЭК 15408-2-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности»

6. 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»

7. ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью»

8. ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»

9. 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»

10. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий»

11. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 «Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер»

12. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети»

13. ГОСТ Р ИСО/ТО 13569-2007 «Финансовые услуги. Рекомендации по информационной безопасности»

14. ГОСТ Р ИСО/МЭК 15026-2002 «Информационная технология. Уровни целостности систем и программных средств»

15. ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности»

16. ГОСТ Р ИСО/МЭК 18045-2008 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий»

17. ГОСТ Р ИСО/МЭК 19794-2-2005 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 2. Данные изображения отпечатка пальца - контрольные точки»

18. ГОСТ Р ИСО/МЭК 19794-4-2006 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 4. Данные изображения отпечатка пальца»

19. ГОСТ Р ИСО/МЭК 19794-5-2006 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица»

20. ГОСТ Р ИСО/МЭК 19794-6-2006 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 6. Данные изображения радужной оболочки глаза»

21. ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования»

22. ГОСТ Р 51188-98 «Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство»

23. ГОСТ Р 51725.6-2002 «Каталогизация продукции для федеральных государственных нужд. Сети телекоммуникационные и базы данных. Требования информационной безопасности»

24. ГОСТ Р 51898-2002 «Аспекты безопасности. Правила включения в стандарты»

25. ГОСТ Р 52069.0-2003 «Защита информации. Система стандартов. Основные положения»

26. ГОСТ Р 52447-2005 «Защита информации. Техника защиты информации. Номенклатура показателей качества»

27. ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»

28. ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»

29. ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хеширования»

30. Стандарт Банка России: «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (СТО БР ИББС-1.0-2008)

31. Стандарт Банка России: «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности» (СТО БР ИББС-1.1-2007)

32. 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)

33. 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)

34. 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)

35. 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)

36. 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 ис-

пользования 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
	измененных	замененных	аннулированных	новых			