МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:
И.о. декана факультета ФиПИ
_____ Таныгин М.О.
(подпись, инициалы, фамилия)
«31» 08 2021 г.

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

Производственная технологическая практика
(наименование вида и типа практики)

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

Безопасность автоматизированных систем
наименование направленности (профиля, специализации)

в сфере информационных и коммуникационных технологий

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

Курск – 2021

Рабочая программа практики составлена в соответствии с:

– федеральным государственным образовательным стандартом высшего образования – бакалавриат по направлению подготовки 10.03.01 «Информационная 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 _____

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

1.1. Цель практики

Целью производственной технологической практики является получение профессиональных умений и опыта профессиональной деятельности в области реализации технологий информационной безопасности.

1.2. Задачи практики

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

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

Вид практики – производственная.

Тип практики –технологическая.

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

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

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

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

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

Форма проведения практики – сочетание дискретного проведения практик по видам и по периодам их проведения.

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

Таблица 2 – Результаты обучения по практике

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за практикой)		*Код и наименование индикатора достижения компетенции, закрепленного за практикой*	*Планируемые результаты обучения по практике, соотнесенные с индикаторами достижения компетенций*
код	*наим*		
ПК-1	Способен эксплуатировать средства обеспечения информационной безопасности автоматизированных систем	ПК-1.1 Производит внедрение в состав автоматизированных систем средств обеспечения информационной безопасности	***Знать:*** - классификацию угроз информационной безопасности (ИБ) в автоматизированных системах (АС); - причины, виды и каналы утечки информации в АС; - способы защиты операционных систем, классификацию систем защиты программного обеспечения (ПО); - методы идентификации и установления подлинности пользователей и объектов, типы аутентификации и межсетевых экранов, способы их реализации; - классификацию компьютерных вирусов, виды антивирусных программ; - средства анализа защищённости АС; - перечень мероприятий по защите информации от вирусов; - этапы внедрения и отладки программно-аппаратных средств защиты информации в АС. ***Уметь:*** - реализовывать контроль доступа средствами АС и аудит потоков данных; - использовать средства аутентификации АС; применять однора-

			зовые пароли, шифрование паролей и данных, определять уязвимые места в прикладном ПО, устанавливать программы защиты приложений, контролировать ресурсы оборудования АС; - использовать антивирусное ПО, специальные средства контроля и фильтрации доступа (сетевые экраны); - использовать средства анализа защищённости АС (сканеры безопасности); -системы обнаружения сетевых атак; применять средства защиты информации в АС, проводить анализ информационных рисков. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками внедрения и отладки программных средств защиты АС; - установки и эксплуатации средств анализа защищённости АС (сканеров безопасности); систем обнаружения сетевых атак; - реализации контроля доступа и аудита, использования антивирусного ПО, настройки специальных средств контроля и фильтрации доступа (сетевых экранов); - определения уязвимых мест в прикладном ПО, контроля ресурсов оборудования АС.
		ПК-1.2 Соотносит функционал автоматизированных систем средств обеспечения информационной безопасности с реализуемыми процедурами обеспечения информационной безопасности	***Знать***: - технические характеристики и особенности функционирования программно-аппаратных средств ЗИ в АС; - перечень и объём мероприятий по обеспечению безопасности и защищённости АС, виды угроз АС, типы, виды, назначение средств защиты информации в АС; - состав, характеристики, назначение, функции оборудования АС; классификацию антивирусного ПО, способы настройки сетевых экранов. ***Уметь:*** **-** проводить анализ угроз, рисков АС, осуществлять выбор оборудо-

			вания и средств защиты АС в соответствии с решаемыми АС задачами, классифицировать средства защиты исходя из функционала АС, определять состав средств защиты для обеспечения выполнения задач АС; - применять программные средства защиты сетевого оборудования, антивирусные программные комплексы, настраивать режимы работы межсетевых экранов. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками анализа функциональных возможностей оборудования и средств защиты АС, технических характеристик сетевого оборудования и программно-аппаратных средств ЗИ в АС; - выбора и эксплуатации средств ЗИ в АС в соответствии с функциональными задачами АС, настройки сетевых экранов, установки ПО, разработки защищённых сайтов.
		ПК-1.3 Выполняет регламентные работы по эксплуатации средств защиты информации	***Знать:*** - типы регламентных работ, классификацию программных и аппаратных средств анализа защищённости АС, систем обнаружения сетевых атак, антивирусного ПО; - технические характеристики и правила эксплуатации средств защиты информации (СЗИ); - эксплуатационную документацию, возможные угрозы и методики определения рисков, порядок настройки сетевого и программного оборудования и режимы функционирования. ***Уметь:*** **-** проводить анализ защищенности АС; - использовать программные и аппаратные средств анализа защищённости АС, системы обнаружения сетевых атак, антивирусное ПО, настраивать межсетевое оборудование. ***Владеть (****или* ***Иметь опыт деятельности):***

			- навыками эксплуатации программных и аппаратных средств анализа защищённости АС, систем обнаружения сетевых атак, антивирусного ПО; - программных средств анализа и управления рисками, навыками настройки сетевых экранов, разработки защищенных сайтов.
		ПК-1.4 Устраняет неисправности при эксплуатации средств защиты информации	***Знат:*** **-** назначение и классификацию программно-аппаратных средств АС; - особенности функционирования ПО АС; классификацию программных и аппаратных средств анализа защищённости АС, систем обнаружения сетевых атак, антивирусного ПО; - технические характеристики и правила эксплуатации средств защиты информации (СЗИ); - эксплуатационную документацию. ***Уметь:*** **-** проводить мониторинг безопасности АС; обнаруживать уязвимые места в функционировании ПО и аппаратного оборудования АС; - провести настройку ПО и оборудования АС. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками настройки программных и аппаратных средств анализа защищённости АС, систем обнаружения сетевых атак, антивирусного ПО; - программных средств анализа и управления рисками, навыками разработки защищенных сайтов.
ПК-2	Способен реализовывать политики безопасности с использованием инструментальных средств обеспечения информационной безопасности	ПК-2.1 Формулирует критерии безопасности обработки информации в автоматизированных системах	***Знать:*** - требования действующих стандартов и рекомендаций, определяющих критерии оценки безопасности АС и этапы анализа рисков и угроз безопасности и уязвимости АС; - классификацию общих критериев, пути организации общих критериев;

			- требования к разработке должностных инструкций; - порядок эксплуатации программно-аппаратных средств защиты АС; - основные принципы построения политики безопасности; - методы и способы защиты информации в АС, методы анализа угроз и оценки рисков информационной безопасности АС. ***Уметь:*** - применять требования действующих стандартов и рекомендаций для обеспечения - безопасности обработки информации в АС; разрабатывать служебную и техническую документацию; - применять средства защиты информации в соответствии с заданными требованиями к АС; - проводить анализ информационных рисков. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками применения требования действующих стандартов и рекомендаций для обеспечения безопасности обработки информации в АС; - разработки служебной и технической документации; программных средств защиты информации, разработки архитектуры сетевой защиты.
		ПК-2.2 Выполняет мероприятия для реализации политики информационной безопасности	***Знать:*** **-** виды угроз и каналы утечки информации, состав, структуру, требования и принципы построения политики безопасности; - модели и типы политик безопасности; - состав, технические характеристики и правила эксплуатации программно-аппаратных средств АС; - основные элементы политики безопасности, методы управления доступом, средства идентификация и аутентификация, анализа регистрационной информации;

			- требования к технической, должностной и эксплуатационной документации; требования к уровням надёжности (безопасности); - основные виды сетевых атак. ***Уметь:*** - проводить анализ угроз, рисков; - разрабатывать документацию пользователя, администратора сети, применять тестовые программы; - разрабатывать архитектуры АС, разрабатывать политики безопасности; применять средства защиты информации в АС, проводить анализ защищенности АС, применять антивирусные программные комплексы, настраивать режимы работы межсетевых экранов. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками разработки документации пользователя, администратора сети, разработки и применения тестовых программ, описания архитектуры, описания политики безопасности; - навыками защиты информации в компьютерных системах, навыками анализа защищенности АС, применения антивирусных программных комплексов, настройки режимов работы межсетевых экранов.
		ПК-2.3 Определяет состав средств, необходимый для управления автоматизированными системами и средствами их защиты от НСД	***Знать:*** - требования руководящих документов по защите АС от НСД; - классификацию средств и АС по уровню защищённости от НСД; - требования к защищённости АС; - показатели и классы защищённости межсетевых экранов от НСД к информации; - классификацию ПО СЗИ, требования руководящих документов к составу и содержанию документаций и испытаний ПО СЗИ; - механизмы управления ключами, шифрованием, администрирования управления доступом, аутентификацией, маршрутизацией; - задачи и методы управления си-

			стемой защиты АС; - типы, состав, назначение, способы применения современных систем управления защитой АС; - показатели защищенности средств вычислительной техники от несанкционированного доступа, классы защищенности автоматизированных систем. ***Уметь:*** **-** проводить анализ защищенности локальной вычислительной сети, определять текущее состояние оборудования АС; - применять программно-аппаратные средства ЗИ в АС; - классифицировать программные продукты управления в соответствии с задачами АС, подбирать конфигурацию системы управления безопасности АС; - проводить анализ информационных рисков. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками определения задач АС, классификации оборудования АС (серверов, АРМ, рабочих станций, сетевое оборудование), - навыками установки ПО серверной и клиентской части, настройки систем управления доступом, эксплуатации программных средств мониторинга и управления средствами безопасности АС; - навыками определения уязвимых мест АС и выбора средств защиты от НСД.
		ПК-2.5 Устанавливает программное обеспечение в соответствии с требованиями по защите информации	***Знать:*** - причины, виды и каналы утечки информации в АС; - способы защиты операционных систем, классификацию систем защиты программного обеспечения (ПО); - типы аутентификации и межсетевых экранов, способы их реализации; -виды антивирусных программ; - средства анализа защищённости АС; - алгоритм установки и отладки

			ПО защиты информации в АС. ***Уметь:*** - устанавливать программы защиты приложений, антивирусное ПО, специальные средства контроля и фильтрации доступа (сетевые экраны); - средства анализа защищённости АС (сканеры безопасности); - системы обнаружения сетевых атак; применять средства защиты информации в АС. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками внедрения и отладки программных средств защиты АС; - установки и эксплуатации средств анализа защищённости АС (сканеров безопасности); - систем обнаружения сетевых атак; - реализации контроля доступа и аудита, установки антивирусного ПО, настройки специальных средств контроля и фильтрации доступа (сетевых экранов), контроля ресурсов оборудования АС.
ПК-3	Способен обеспечивать безопасную обработку данных в автоматизированных системах	ПК-3.1 Фиксирует возникновение инцидентов информационной безопасности	***Знать:*** - понятие инцидент; - классификация и параметры инцидентов информационной безопасности; - регламенты, определяющие порядок управления инцидентами информационной безопасности; - принципы управления инцидентами. ***Уметь:*** - определить тип инцидента; - зарегистрировать инцидент информационной безопасности; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками определения типа инцидента; - навыками управления инцидентами информационной безопасности.
		ПК-3.2 Использует методы и средства резервного копирова-	***Знать:*** - методы резервного копирования информации;

		ния информации	- типы и характеристики носителей хранения данных; - типы и характеристики используемых платформ; - схемы копирования; - базовые функции резервного копирования информации. ***Уметь:*** - определить необходимый тип носителя хранения данных; - использовать оптимальную схему копирования; - применить оптимальный тип резервного копирования. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками выбора необходимой для копирования информации; - навыками организации процесса резервного копирования.
		ПК-3.3 Устраняет уязвимости в автоматизированной системе	***Знать:*** - понятие уязвимости, классификация уязвимостей в автоматизированной системе; - поисковые признаки; - методы оценки опасности угроз; - методы устранения угроз. ***Уметь:*** - анализировать уязвимости в автоматизированной системе; - выбрать средства для поиска уязвимостей; - устранять уязвимости в автоматизированной системе. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками анализа уязвимости в автоматизированной системе; - навыками поиска уязвимости; - навыками устранения уязвимости в автоматизированной системе.
		ПК-3.4 Соотносит изменения в конфигурации автоматизированной системы с её защищенностью	***Знать:*** - основные методы управления защитой информации; - основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; - методы защиты информации от "утечки" по техническим каналам; - нормативные правовые акты в области защиты информации

			Уметь: - анализировать воздействия изменений конфигурации автоматизированной системы на ее защищенность; - оценивать информационные риски в автоматизированных системах - классифицировать и оценивать угрозы безопасности информации - конфигурировать параметры системы защиты информации автоматизированных систем - применять технические средства контроля эффективности мер защиты информации. ***Владеть (или Иметь опыт деятельности):*** **-** навыками анализа, оценки информационных рисков в автоматизированных системах; - навыками настройки системы защиты информации.
ПК-6	Способен документально оформлять работы по обеспечению информационной безопасности	ПК-6.1 Анализирует полноту и соответствие нормативным требованиям руководящих документов, описывающих работы по обеспечению информационной безопасности	***Знать:*** - основные нормативно-правовые акты в области информационной безопасности и защиты информации; - правовые основы организации защиты государственной тайны и конфиденциальной информации; ***Уметь:*** - анализировать полноту и соответствие нормативным требованиям руководящих документов, описывающих работы по обеспечению информационной безопасности. ***Владеть (или Иметь опыт деятельности):*** - навыками составления перечня руководящих документов, описывающих требования к информационной безопасности; - навыками анализа требований руководящих документов.
		ПК-6.2 Формирует отчётные и руководящие документы для обеспечения защиты информации в информационной систе-	***Знать:*** -основные нормативно-правовые акты в области информационной безопасности и защиты информации; - содержание и порядок деятель-

		ме в ходе ее эксплуатации	ности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности информационных систем; -основные методы организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации. ***Уметь:*** - оформлять документацию по регламентации процесса эксплуатации информационной системы с целью обеспечения защиты информации; - оформлять отчётную и техническую документацию в соответствии с действующими нормативными документами; ***Владеть (или Иметь опыт деятельности):*** - навыками составления отчётной и технической документации, описывающей требования к информационной безопасности; - навыками ведения протоколов и журналов учета при изменении конфигурации, осуществлении аудита и мониторинга систем защиты информации информационных систем.
		ПК-6.3 Формулирует в соответствии с требованиями руководящих документов состав и содержание процедур контроля обеспеченности уровня защищенности информации	***Знать:*** -основные нормативно-правовые акты в области информационной безопасности и защиты информации; -методы обеспечения уровня защищённости информации; - принципы построения систем защиты информации. ***Уметь:*** - классифицировать и оценивать угрозы безопасности информации для объекта информатизации - разрабатывать процедуры контроля обеспеченности уровня защищённости информации; - применять действующую законодательную базу в области обеспечения защиты информации ***Владеть (или Иметь опыт деятельности):***

			- основными криптографическими методами, алгоритмами, протоколами, используемых для обеспечения безопасности информации; - способами и средствами защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; - принципами построения систем защиты информации.
		ПК-6.4 Готовит документы для проведения работ по аттестации объектов информатизации и автоматизированных систем	***Знать:*** - порядок организации и проведения аттестации объектов информатизации и информационных систем (ИС); - условия функционирования объектов и ИС; -основные нормативно-правовые акты в области информационной безопасности и защиты информации. ***Уметь:*** - проверять организационно распорядительную документации по защите информации; - проводить испытания объектов информатизации на соответствие требованиям по защите конфиденциальной информации от утечки; - готовить документы для проведения работ по аттестации объектов информатизации и ИС. ***Владеть (или Иметь опыт деятельности):*** - навыками анализа необходимой документации; - навыками проведения испытаний объектов информатизации и ИС; - навыками подготовки документации для проведения работ по аттестации объектов информатизации и ИС.

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

Производственная технологическая практика входит в часть, формируемую участниками образовательных отношений, блока 2 «Практика» основной профессиональной образовательной программы – программы специалитета 10.05.02 Информационная безопасность телекоммуникационных систем, специализация «Управление безопасностью телекоммуникационных систем и сетей». Практика проходит на 6 курсе в 11 семестре.

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

4 Содержание практики

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

Контактная работа по практике (включая контактную работу по промежуточной аттестации по практике) составляет 24 часа (часы указаны в учебном плане в графе «Пр»), работа обучающегося в иных формах – 192 часов (часы указаны в учебном плане в графе «СР»).

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

Таблица 4 – Этапы и содержание практики

№ п/п	Этапы практики	Содержание практики	Трудоемкость (час)
1	Подготовительный этап	Решение организационных вопросов: 1) распределение обучающихся по местам практики; 2) знакомство с целью, задачами, программой, порядком прохождения практики; 3) получение заданий от руководителя практики от университета; 4) информация о требованиях к отчетным документам по практике; 5) первичный инструктаж по тех-	2

		нике безопасности.	
2	Основной этап	Работа обучающихся в профильной организации	108
2.1	Знакомство с профильной организацией	Знакомство с профильной организацией, руководителем практики от организации, рабочим местом и должностной инструкцией.	2
		Инструктаж по технике безопасности на рабочем месте.	5
		Знакомство с содержанием деятельности профильной организации по обеспечению информационной безопасности и проводимыми в нем мероприятиями.	
		Изучение нормативных правовых актов профильной организации по обеспечению информационной безопасности (политика безопасности профильной организации, положения, приказы, инструкции, должностные обязанности, памятки и др.).	3
2.2	Практическая подготовка обучающихся *(непосредственное выполнение обучающимися видов работ, связанных с будущей профессиональной деятельностью)*	Самостоятельное проведение мониторинга и (или) производственного контроля эффективности применения средств защиты информации в ТКС. Организация работы 2-3 человек и руководство их работой в процессе формулирования предложений по совершенствованию системы защиты информации в ТКС. Создание плана работы коллектива из 3 – 4 человек, реализующего политику безопасности в ТКС	60.

		Самостоятельная обработка и систематизация полученных данных с помощью средств проектирования и выполнения технико-экономических расчетов. *Организация работы 2-3 человек и руководство их работой в процессе обработки и систематизации полученных данных.* Представление результатов мониторинга руководителю практики от организации	15
		Самостоятельное проведение анализа результатов проведенного мониторинга информационной безопасности. Организация работы 2-3 человек и руководство их работой в процессе работ по разработки систем защиты информации. Оценка эффективности применения средств информационной безопасности. Представление результатов анализа и обоснование оценки руководителю практики от организации.	
		Самостоятельная подготовка рекомендаций по повышению уровня информационной безопасности предприятия. *Организация работы 2-3 человек и руководство их работой в процессе подготовки рекомендаций по повышению уровня информационной безопасности предприятия.* Представление своих рекомендаций руководителю практики от организации.	
3	Заключительный этап	Оформление дневника практики.	36
		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
ПК-2	Математическое моделирование технических систем	Производственная проектно-технологическая практика	
ПК-3	Управление разработкой систем безопасности	Методы и средства пространственного анализа Методы пространственного моделирования радиоканала	Производственная проектно-технологическая практика
ПК-4	Управление разработкой систем безопасности	Производственная проектно-технологическая практика	
ПК-5	Квантовая и оптическая электроника Контроль защищённости информационно-телекоммуникационных систем		Производственная проектно-технологическая практика

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

Таблица 6.2 – Показатели и критерии оценивания компетенций, шкала оценивания

Код	Показатели	Критерии и шкала оценивания компетенций

компетенции/ этап *(указывается название этапа из п.6.1)*	оценивания компетенций *(индикаторы достижения компетенций, закрепленные за практикой)*	Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
ПК-2/ завершающий	ПК-2.1 Определяет численные характеристики моделируемых систем	**Знать**: терминологию предметной области математического моделирования **Уметь**: Использовать различные подходы к классификации процессов в области ИБ **Владеть навыками**: Навыками использования различных методологических подходов в анализе прикладных и фундаментальных задач	**Знать**: основные фундаментальные положения теории математического и численного моделирования. **Уметь**: сопоставлять фундаментальные положения теории математического моделирования реальным задачам **Владеть навыками**: анализа объекта исследования с точки зрения возможности описания его математическим языком	**Знать**: номенклатуру методов и средств проведения математических экспериментов **Уметь**: проводить математический эксперимент и оценивать его достоверность **Владеть навыками**: проведения математического эксперимента
	ПК-2.2 Оптимизирует параметры моделируемых систем с целью достижения целевых показателей функционирования	**Знать**: основные характеристики технических систем и систем управления **Уметь**: получать характеристики систем по результатам математических экспериментов **Владеть навыками**: элементарного манипулирования моделируемыми параметрами с целью достижения требуемого результата моделирования	**Знать**: критерии эффективности применяемых средств и решений **Уметь**: достигать требуемых целевых значений математических экспериментов **Владеть навыками**: целенаправленного манипулирования моделируемыми параметрами с целью достижения требуемого результата моделирования	**Знать**: методы определения диапазонов параметров работающих систем для достижения целевого результата **Уметь**: оптимизировать параметры моделируемой системы **Владеть навыками**: самостоятельного выбора диапазонов значений моделируемых параметров с целью достижения требуемого результата моделирования
	ПК-2.3 Формирует технические	**Знает:** Основные функциональные зависи-	**Знает:** методологию установления зависи-	**Знает:** законы, технологий, правила, при-

1	2	3	4	5
	решения, направленные на улучшение существующих методов защиты информации в телекоммуникационных системах	мости между параметрами систем и показателями их функционирования.. **Умеет:** Оформлять и представлять результаты анализа зависимостей между параметрами и характеристиками технических систем. **Владеет:** элементарными навыками оформления полученных в результате экспериментов результатов.	мостей между параметрами систем и показателями их функционирования. ***Уметь:*** изменять целевые характеристики функционирования телекоммуникационных систем за счёт изменения параметров их работы ***Владеть (или Иметь опыт деятельности):*** базовыми навыками обоснования решений, направленных улучшение существующих методов защиты информации	емы манипулирования параметрами технических систем с целью достижения целевых показателей функционирования. **Умеет:** Способен самостоятельно обработать, проанализировать и представить Внедрения решений, направленных на улучшение существующих методов защиты информации . **Владеет:** навыками научного обоснования решений, направленных улучшение существующих методов защиты информации
ПК-3 завершающий	ПК-3.1 Оценивает эффективности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик	***Знать:*** номенклатуру стандартов и рекомендаций, определяющих критерии оценки безопасности ТКС. ***Уметь:*** применять требования действующих стандартов при обработке информации в ТКС. ***Владеть:*** навыками обеспечения безопасности обработки информации в ТКС.	***Знать:*** требования отечественных стандартов и рекомендаций, определяющих критерии оценки безопасности ТКС и этапы анализа рисков и угроз безопасности и уязвимости ТКС. ***Уметь:*** применять требования действующих стандартов и рекомендаций для обеспечения безопасности обработки информации в ТКС. ***Владеть:*** навыками имплементации требований действующих стандартов и рекомендаций для обеспечения	***Знать:*** требования отечественных и мировых стандартов и рекомендаций, определяющих критерии оценки безопасности ТКС и этапы анализа рисков и угроз безопасности и уязвимости ТКС. ***Уметь:*** грамотно применять требования действующих стандартов и рекомендаций для построения эффективных систем безопасности в ТКС. ***Владеть:*** уверенными навыками использования требований действу-

1	2	3	4	5
			безопасности обработки информации в ТКС.	ющих стандартов и рекомендаций для обеспечения безопасности обработки информации в ТКС.
	ПК-3.2 Оценивает соответствие механизмов безопасности системы требованиям нормативных документов и рискам	***Знать***: виды угроз ТКС, состав, характеристики, назначение, функции оборудования ТКС. ***Уметь:*** использовать оборудование и средства защиты ТКС в соответствии с решаемыми ТКС задачами. ***Владеть :*** работы с оборудованием и средствами защиты ТКС.	***Знать***: виды угроз ТКС, типы, виды, назначение средств защиты информации в ТКС; состав, характеристики, назначение, функции оборудования ТКС; классификацию антивирусного ПО. ***Уметь:*** проводить выбор оборудования и средств защиты ТКС в соответствии с решаемыми ТКС задачами. ***Владеть :*** навыками определения функциональных возможностей оборудования и средств защиты ТКС.	***Знать***: виды угроз ТКС, типы, виды, назначение средств защиты информации в ТКС; состав, характеристики, назначение, функции оборудования ТКС; классификацию антивирусного ПО, способы настройки сетевых экранов. ***Уметь:*** проводить обоснованный выбор оборудования и средств защиты ТКС в соответствии с нетиповыми задачами. ***Владеть :*** навыками анализа функциональных возможностей оборудования и средств защиты ТКС.
	ПК-3.3 Формулирует критерии оценки эффективности механизмов безопасности, используемых в телекоммуникационных системах	***Знать:*** критерии оценки эффективности механизмов безопасности телекоммуникационных систем. ***Уметь:*** применять средства защиты информации в соответствии с отдельными требованиями к ТКС. ***Владеть:*** навыками фиксации результатов применения требований стандартов и рекомендаций для обеспечения без-	***Знать:*** критерии оценки эффективности механизмов безопасности телекоммуникационных систем и этапы анализа рисков и угроз безопасности и уязвимости ТКС. ***Уметь:*** применять средства защиты информации в соответствии с заданными требованиями к ТКС. ***Владеть:*** навыками оценки эффекта от применения требований стандартов	***Знать:*** методы оценки эффективности механизмов безопасности телекоммуникационных систем и этапы анализа рисков и угроз безопасности и уязвимости ТКС. ***Уметь:*** формировать методику применения средства защиты информации в соответствии с заданными требованиями к ТКС. ***Владеть:*** навыками комплексной

1	2	3	4	5
		опасности обработки информации в ТКС.	и рекомендаций для обеспечения безопасности обработки информации в ТКС.	оценки эффективности применения требований стандартов и рекомендаций для обеспечения безопасности обработки информации в ТКС.
	ПК-3.4 Формулирует предложения по повышению эффективности механизмов безопасности, используемых в телекоммуникационных системах	***Знать:*** состав, типовых телекоммуникационных систем предприятий и организаций. ***Уметь:*** определять характеристики, решаемых задач компонентов ИС прикладного характера, системного и прикладного ПО, обеспечивающего функционирование ТКС. ***Владеть:*** определять характеристики технических средств и оборудования из состава телекоммуникационных систем, оценки предлагаемых к реализации вариантов построения телекоммуникационных систем.	***Знать:*** конфигурацию, состав, структуру, принципы функционирования типовых телекоммуникационных систем предприятий и организаций. ***Уметь:*** сопоставлять состав, технических характеристик, решаемых задач компонентов ИС прикладного характера, системного и прикладного ПО, обеспечивающего функционирование ТКС. ***Владеть:*** навыками сравнительного анализа технических средств и оборудования из состава телекоммуникационных систем, оценки предлагаемых к реализации вариантов построения телекоммуникационных систем.	***Знать:*** конфигурацию, состав, структуру, принципы функционирования нетиповых телекоммуникационных систем предприятий и организаций. ***Уметь:*** проводить сравнительный анализ состава, технических характеристик, решаемых задач компонентов ИС прикладного характера, системного и прикладного ПО, обеспечивающего функционирование ТКС. ***Владеть:*** навыками глубокого и обоснованного анализа технических средств и оборудования из состава телекоммуникационных систем, оценки предлагаемых к реализации вариантов построения телекоммуникационных систем.
ПК-4/ завершающий	ПК-4.1 Разрабатывает проектные документы на средства защиты ин-	***Знать***: состав материально технической базы необходимой для разработки программно-аппаратных средств.	***Знать***: состав материально технической базы необходимой для разработки программно-аппаратных средств, порядок	***Знать***: состав материально технической и лабораторной базы необходимой для разработки программно-аппаратных

1	2	3	4	5
	формации создаваемых телекоммуникационных систем и сетей	***Уметь:*** использовать отдельные элементы оборудования необходимыми для выполнения работ по проектированию ТКС. ***Владеть:*** навыками работы с отдельными инструментами и оборудованием необходимыми для выполнения работ по проектированию ТКС.	разработки и согласования расчётно-калькуляционных материалов проекта по разработке ТКС. ***Уметь:*** использовать инструменты и оборудование необходимыми для выполнения работ по проектированию ТКС. ***Владеть:*** навыками работы с инструментами и оборудованием необходимыми для выполнения работ по проектированию ТКС.	средств, сборки и монтажа сетевого оборудования ТКС; порядок разработки и согласования расчётно-калькуляционных материалов проекта по разработке ТКС. ***Уметь:*** управлять инструментами и оборудованием необходимыми для выполнения работ по проектированию ТКС. ***Владеть:*** навыками подбора и работы с инструментами и оборудованием, необходимыми для выполнения работ по проектированию ТКС.
	ПК-4.2 Готовит техническую и проектную документацию по вопросам создания и эксплуатации телекоммуникационных систем и сетей	***Знать:*** порядок внедрения, отладки и развития процессов и этапов разработки требований, задач. ***Уметь:*** отлаживать этапы работ обеспечения информационной безопасности защищённых ТКС в процессе их эксплуатации и модернизации. ***Владеть:*** навыками отладки систем обеспечения информационной безопасности ТКС в процессе их эксплуатации и модернизации.	***Знать:*** порядок внедрения, отладки и развития процессов и этапов разработки требований, задач, критериев качества информационной безопасности защищённых ТКС в процессе их эксплуатации и модернизации. ***Уметь:*** управлять внедрением, отладкой и развитием процессов и этапов работ, методов обеспечения информационной безопасности защищённых ТКС в процессе их эксплуатации и модернизации. ***Владеть:*** навыками управления внедрением, отлад-	***Знать:*** порядок внедрения, отладки и развития процессов и этапов разработки требований, задач, критериев качества и методов обеспечения информационной безопасности защищённых ТКС в процессе их эксплуатации и модернизации. ***Уметь:*** организовать и управлять внедрением, отладкой и развитием процессов и этапов работ, методов обеспечения информационной безопасности защищённых ТКС в процессе их эксплуатации и модернизации.

1	2	3	4	5
			кой и развитием процессами и этапами разработки системобеспечения информационной безопасности ТКСв процессе их эксплуатации и модернизации.	***Владеть:*** навыками организации и управления внедрением, отладкой и развитием процессами и этапами разработки систем обеспечения информационной безопасности ТКСв процессе их эксплуатации и модернизации.
	ПК-4.3 Проводит аттестацию программ и алгоритмов на предмет соответствия требованиям защиты информации	***Знать:*** возможные каналы утечки информации, основы построения политики информационной безопасности, технические характеристики. ***Уметь:*** определять отдельные характеристики алгоритмов и программных средств защиты информации. ***Владеть:*** навыками определения отдельных характеристик алгоритмов и программных средств защиты информации на предмет соответствия требованиям защищённых ТКС.	***Знать:*** виды угроз и основные каналы утечки информации, основные принципы построения политики информационной безопасности. ***Уметь:*** определять характеристики алгоритмов и программных средств защиты информации. ***Владеть:*** навыками определения характеристик алгоритмов и программных средств защиты информации.	***Знать:*** виды угроз и все возможные каналы утечки информации, основные принципы построения политики информационной безопасности. ***Уметь:*** проводить анализ алгоритмов и программных средств защиты информации на предмет соответствия требованиям защищённых ТКС. ***Владеть:*** навыками анализа алгоритмов и программных средств защиты информации на предмет соответствия требованиям защищённых ТКС.
	ПК-4.4 Производит сравнительный анализ вариантов конфигураций и состава телекоммуникационных систем и сетей	***Знать:*** основные требования к системам защиты информации; классы защищенности автоматизированных систем ***Уметь:*** проводить отдельные этапы сравнительного анализа состава и конфигурации ТКС, в том числе	***Знать:*** основные требования к системам защиты информации; показатели защищенности средств вычислительной техники от несанкционированного доступа, классы защищенности автоматизированных систем; ТКС, в том числе	***Знать:*** основные требования к системам защиты информации; показатели защищенности средств вычислительной техники от несанкционированного доступа, классы защищенности автоматизированных систем; этапы сравнитель-

1	2	3	4	5
		покупных и вновь разрабатываемых программных и аппаратных средств ТКС. ***Владеть:*** навыками проведения отдельных этапов сравнительного анализа состава и конфигурации ТКС.	номенклатуру покупных и вновь разрабатываемых программных и аппаратных средства ТКС. ***Уметь:*** проводить основные этапы сравнительного анализа состава и конфигурации ТКС, в том числе покупных и вновь разрабатываемых программных и аппаратных средств ТКС. ***Владеть:*** навыками проведения основных этапов сравнительного анализа состава и конфигурации ТКС, в том числе покупных и вновь разрабатываемых программных и аппаратных средств ТКС.	ного анализа состава и конфигурации ТКС, в том числе номенклатуру покупных и вновь разрабатываемых программных и аппаратных средства ТКС. ***Уметь:*** проводить сравнительный анализ состава и конфигурации ТКС, в том числе покупных и вновь разрабатываемых программных и аппаратных средств ТКС. ***Владеть:*** навыками проведения сравнительного анализа состава и конфигурации ТКС, в том числе покупных и вновь разрабатываемых программных и аппаратных средств ТКС.
ПК-5/ завершающий	ПК-5.1 Разрабатывает методику оценки уровня защищённости телекоммуникационной системы	***Знать:*** номенклатуру этапов работ по оценке уровня защищённости телекоммуникационной системы ***Уметь:*** проводить оценку отдельных характеристик защищённости телекоммуникационной системы ***Владеть (или Иметь опыт деятельности):*** навыками оценки отдельных характеристик телекоммуникационной системы	***Знать:*** последовательность работ по оценке уровня защищённости телекоммуникационной системы ***Уметь:*** проводить оценку уровня защищённости телекоммуникационной системы ***Владеть (или Иметь опыт деятельности):*** навыками контроля уровня защищённости телекоммуникационной системы	***Знать:*** методику и принципы оценки уровня защищённости телекоммуникационной системы ***Уметь:*** проводить оценку уровня защищённости сложной и нетиповой телекоммуникационной системы ***Владеть (или Иметь опыт деятельности):*** навыками контроля уровня защищённости сложной и нетиповой телекоммуникационной системы

1	2	3	4	5
	ПК-5.2 Проводит оценку соответствия уровня защищённости требованиям политики безопасности и нормативным документам	***Знать:*** отдельные требования нормативных документов, предъявляемые к ТКС ***Уметь:*** определять отдельные количественные и качественные показатели защищённости ТКС в соответствии с требованиям нормативных документов ***Владеть (****или* ***Иметь опыт деятельности):*** определения отдельных количественных и качественных показателей в соответствии с требованиям политики безопасности и нормативным документов	***Знать:*** основные требования нормативных документов, предъявляемые к ТКС ***Уметь:*** определять текущие количественные и качественные показатели защищённости ТКС в соответствии с требованиям нормативных документов ***Владеть (****или* ***Иметь опыт деятельности):*** определения текущих количественных и качественных показателей в соответствии с требованиям политики безопасности и нормативным документов	***Знать:*** все требования нормативных документов, предъявляемые к ТКС ***Уметь:*** соотносить текущие количественные и качественные показатели защищённости ТКС требованиям нормативных документов ***Владеть (****или* ***Иметь опыт деятельности):*** навыками оценки соответствия уровня защищённости требованиям политики безопасности и нормативным документам
	ПК-5.3 Разрабатывает систему мероприятий по оценке уровня защищённости телекоммуникационной системы	***Знать:*** отдельные количественные и качественные показатели защищённости ТКС ***Уметь:*** использовать инструментальные средства для определения количественных и качественных показателей защищённости ТКС ***Владеть (****или* ***Иметь опыт деятельности):*** проведения отдельных действий по определению количественных и качественных показателей защищённости ТКС	***Знать:*** основные количественные и качественные показатели защищённости ТКС ***Уметь:*** с помощью инструментальных средств определять количественных и качественных показателей защищённости ТКС ***Владеть (****или* ***Иметь опыт деятельности):*** формированию последовательности действий по определению количественных и качественных показателей защищённости ТКС	***Знать:*** количественные и качественные показатели защищённости ТКС ***Уметь:*** определять количественных и качественных показателей защищённости ТКС комбинацией различных методов и средств ***Владеть (****или* ***Иметь опыт деятельности):*** систематизации действий по определению количественных и качественных показателей защищённости ТКС
	ПК-5.4 Определяет	***Знать:*** отдельные уязвимости защи-	***Знать:*** уязвимости защищённости те-	***Знать:*** уязвимости защищённости те-

1	2	3	4	5
	уязвимости защищённости телекоммуникационных систем и сетей	щённости телекоммуникационных систем и сетей и угрозы ТКС ***Уметь:*** использовать инструментальные средства выявления уязвимостей защищённости телекоммуникационных систем и сетей ***Владеть (или Иметь опыт деятельности):*** навыками выявления типовых уязвимостей защищённости телекоммуникационных систем и сетей	лекоммуникационных систем и сетей и угрозы ТКС ***Уметь:*** с помощью инструментальных средств выявлять уязвимости защищённости телекоммуникационных систем и сетей ***Владеть (или Иметь опыт деятельности):*** навыками выявления уязвимостей защищённости телекоммуникационных систем и сетей	лекоммуникационных систем и сетей и угрозы ТКС и методики их выявления ***Уметь:*** выявлять уязвимости защищённости телекоммуникационных систем и сетей комбинацией различных методов и средств ***Владеть (или Иметь опыт деятельности):*** навыками выявления уязвимостей защищённости телекоммуникационных систем и сетей, в том числе и не описанных в специализированных справочниках

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
ПК-2 завершающий	Дневник практики. Отчёт по практике с научно-обоснованными решениями по увеличению защищённости телекоммуникационных систем и сетей Доклад обучающегося на промежуточной аттестации (защита отчета о практике). Характеристика руководителя практики от организации управленческих качеств обучающегося.
ПК-3	Дневник практики.

завершающий	Отчет о практике. Типовое задание № 1 по практической подготовке, предусматривающее выполнение обучающимся вида(ов) работ, связанного(ых) с будущей профессиональной деятельностью (задание конкретизируется с учетом особенностей конкретной профильной организации в Дневнике практики, в п.1.4 задания студенту): *Сформируйте 4 критерия эффективности применения средств обеспечения ИБ в ТКС, произведите шкалирование критериев и сформируйте итоговую оценку эффективнсти использованных на рельном объекте решений.* Ответы на вопросы по содержанию практики на промежуточной аттестации.
ПК-4 завершающий	Дневник практики. Отчет о практике. Типовое задание № 2 по практической подготовке, предусматривающее выполнение обучающимся вида(ов) работ, связанного(ых) с будущей профессиональной деятельностью (задание конкретизируется с учетом особенностей конкретной профильной организации в Дневнике практики, в п.1.4 задания студенту): *Исходя из сформированных критериев предложите проектные, организационные и иные решения для повышения эффективности системы защиты.* Доклад обучающегося на промежуточной аттестации (защита отчета о практике). Характеристика руководителя практики от организации управленческих качеств обучающегося.
ПК-5 завершающий	Дневник практики. Типовое задание № 3 по практической подготовке, предусматривающее выполнение обучающимся вида(ов) работ, связанного(ых) с будущей профессиональной деятельностью (задание конкретизируется с учетом особенностей конкретной профильной организации в Дневнике практики, в п.1.4 задания студенту): *Разработайте рекомендации по повышению уровня безопасности предприятия, основываясь на результатах проведенного мониторинга защищённости.* 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.

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 прак-

тикой, 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	Полнота, точность, аргументированность ответов,	4

	на практике) 4 балла		

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

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

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

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

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

Основная литература:

1. Информационная безопасность и защита информации [Текст] : учебное пособие / Ю. Ю. Громов [и др.]. - Старый Оскол : ТНТ, 2013. - 384 с.
2. Нестеров, С. А. Основы информационной безопасности : учебное пособие / С. А. Нестеров ; Санкт-Петербургский государственный политехнический университет. - СПб. : Издательство Политехнического университета, 2014. - 322 с. - URL: http://biblioclub.ru/index.php?page=book&id=363040 (дата обращения 02.09.2021) . - Режим доступа: по подписке. - Текст : электронный.
3. Степанова, Е. Е. Информационное обеспечение управленческой деятельности [Текст] : учебное пособие / Е. Е. Степанова, Н. В. Хмелевская. - М. : Фо-рум, 2004. - 154 с.

Дополнительная литература:

4) Аверченков, В. И. Аудит информационной безопасности [Электронный ресурс] : учебное пособие для вузов / В. И. Аверченков. - 3-е изд., стереотип. - М. : Флинта, 2016. - 269 с. - URL: http://biblioclub.ru/index.php?page=book&id=93245 (дата обращения 02.09.2021) . - Режим доступа: по подписке. - Текст : электронный.

5) Абрамов, Г. В. Проектирование информационных систем : учебное пособие / Г. В. Абрамов, И. Медведкова, Л. Коробова. - Воронеж : Воронежский государственный университет инженерных технологий, 2012. - 172 с. -

URL: http://biblioclub.ru/index.php?page=book&id=141626 (дата обращения 03.09.2021) . - Режим доступа: по подписке. - ISBN 978-5-89448-953-7. - Текст : электронный.

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

7) Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю. Н. Загинайлов. - М. ; Берлин : Директ-Медиа, 2015. - 253 с. - URL: http://biblioclub.ru/index.php?page=book&id=276557 (дата обращения 31.08.2021) . - Режим доступа: по подписке. - Текст : электронный.

8) Куль, Т. П. Операционные системы : учебное пособие / Т. П. Куль. - Минск : РИПО, 2015. - 312 с. - URL: http://biblioclub.ru/index.php?page=book&id=463629 (дата обращения 02.09.2021) . - Режим доступа: по подписке. - Текст : электронный.

9) Лопин, В. Н. Защита информации в компьютерных системах [Текст] : учебное пособие / В. Н. Лопин, И. С. Захаров, А. В. Николаев ; Министерство образования и науки Российской Федерации, Курский государственный технический университет. - Курск : КГТУ, 2006. - 159 с.

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

11) Петренко, В .И. Теоретические основы защиты информации : учебное пособие / В. И. Петренко ; Северо-Кавказский федеральный университет. - Ставрополь : СКФУ, 2015. - 222 с. - URL: http://biblioclub.ru/index.php?page=book&id=458204 (дата обращения 02.09.2021) . - Режим доступа: по подписке. - Текст : электронный.

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

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

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

15) ГОСТ Р ИСО/МЭК 15408-1-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель»

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

17) ГОСТ Р ИСО/МЭК 15408-3-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности»

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

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

20) ГОСТ Р ИСО/МЭК 13335-1-2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий»

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

43) Стандарт Банка России: «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям стандарта СТО БР ИББС-1.0-2008» (СТО БР ИББС-1.2-2009)

44) Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС-1.0» (РС БР ИББС-2.0-2007)

45) Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Руководство по самооценке соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям стандарта СТО БР ИББС-1.0» (РС БР ИББС-2.1-2007)

46) Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности» (РС БР ИББС-2.2-2009)

47) Описание формы предоставления результатов оценки уровня информационной безопасности организаций банковской системы Российской Федерации

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

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

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

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

9 Описание материально-технической базы, необходимой для проведения практики

Для проведения практики используется оборудование конкретной профильной организации, на базе которой она проводится: современная измерительная техника: устройства, позволяющие осуществлять контроль защищённости, программные и аппаратные системы защиты информации, обрабатываемых в телекоммуникационных системах, и устройства, позволяющие фиксировать параметры микроклимата (м*ежсетевые экраны, роутеры, маршрутизаторы, коммутаторы, системы виброакустического зашумления, датчики , акустические излучатели, подавители «жучков» и беспроводных видеокамер , поисковые приборы, генераторы шума*);

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

м*ежсетевые экраны, роутеры, маршрутизаторы, коммутаторы, системы виброакустического зашумления, датчики , акустические излучатели,*

подавители «жучков» и беспроводных видеокамер , поисковые приборы, генераторы шума

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

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

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

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

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

Определение места практики

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

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

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

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

– *для инвалидов по зрению-слабовидящих:* оснащение специального рабочего места общим и местным освещением, обеспечивающим беспрепятственное нахождение указанным лицом своего рабочего места и выполнение трудовых функций, видеоувеличителями, лупами;

– *для инвалидов по зрению-слепых*: оснащение специального рабочего места тифлотехническими ориентирами и устройствами, с возможностью использования крупного рельефно-контрастного шрифта и шрифта Брайля, акустическими навигационными средствами, обеспечивающими беспрепятственное нахождение указанным лицом своего рабочего места и выполнение трудовых функций;

– *для инвалидов по слуху-слабослышащих*: оснащение (оборудование) специального рабочего места звукоусиливающей аппаратурой, телефонами громкоговорящими;

– *для инвалидов по слуху-глухих*: оснащение специального рабочего места визуальными индикаторами, преобразующими звуковые сигналы в световые, речевые сигналы в текстовую бегущую строку, для беспрепятственного нахождения указанным лицом своего рабочего места и выполнения работы;

– *для инвалидов с нарушением функций опорно-двигательного аппарата*: оборудование, обеспечивающее реализацию эргономических принципов (максимально удобное для инвалида расположение элементов, составляющих рабочее место), механизмами и устройствами, позволяющими изменять высоту и наклон рабочей поверхности, положение сиденья рабочего стула по высоте и наклону, угол наклона спинки рабочего стула, оснащение специальным сиденьем, обеспечивающим компенсацию усилия при вставании, специальными приспособлениями для управления и обслуживания этого оборудования.

Особенности содержания практики

Индивидуальные задания формируются руководителем практики от университета с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья каждого конкретного обучающегося данной категории и должны соответствовать требованиям выполнимости и посильности.

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

Особенности организации трудовой деятельности обучающихся

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

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

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

Особенности руководства практикой

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

– учебно-методическую и психолого-педагогическую помощь и контроль со стороны руководителей практики от университета и от организации;

– корректирование (при необходимости) индивидуального задания и программы практики;

– помощь ассистента (ассистентов) и (или) волонтеров из числа обучающихся или работников профильной организации. Ассистенты/волонтеры оказывают обучающимся данной категории необходимую техническую помощь при входе в здания и помещения, в которых проводится практика, и выходе из них; размещении на рабочем месте; передвижении по помещению, в котором проводится практика; ознакомлении с индивидуальным заданием и его выполнении; оформлении дневника и составлении отчета о практике; общении с руководителями практики.

Особенности учебно-методического обеспечения практики

Учебные и учебно-методические материалы по практике представляются в различных формах так, чтобы инвалиды с нарушениями слуха получали информацию визуально (программа практики и индивидуальное задание на практику печатаются увеличенным шрифтом; предоставляются видеоматериалы и наглядные материалы по содержанию практики), с нарушениями зрения – аудиально (например, с использованием программ-синтезаторов речи) или с помощью тифлоинформационных устройств.

Особенности проведения текущего контроля успеваемости и промежуточной аттестации

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

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

11 Лист дополнений и изменений, внесенных в программу практики

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