МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:
Декан факультета
(наименование ф-та, полностью)
фундаментальной и прикладной информатики
_____ Таныгин М.О.
(подпись, инициалы, фамилия)
«31» 08 2021 г.

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

Производственная преддипломная практика
(наименование вида и типа практики)

ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем
шифр и наименование направление подготовки (специальности)

Управление безопасностью телекоммуникационных систем и сетей
наименование направленности (профиля, специализации)

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

Курск – 2021

Рабочая программа практики составлена в соответствии с:

– федеральным государственным образовательным стандартом высшего образования – специалитет по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем», утвержденного приказом Министерства образования и науки Российской Федерации от 26 ноября 2020 г. №1458;

– ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специализация «Управление безопасностью телекоммуникационных систем и сетей», 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 10.05.02 Информационная безопасность телекоммуникационных систем, специализация «Управление безопасностью телекоммуникационных систем и сетей» 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 10.05.02 Информационная безопасность телекоммуникационных систем на основании учебного плана ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специализация «Управление безопасностью телекоммуникационных систем и сетей», одобренного Ученым советом университета протокол №6 «22» 02 20 21 г., на заседании кафедры ИБ протокол № 11 от 30.06.2022.

(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 10.05.02 Информационная безопасность телекоммуникационных систем на основании учебного плана ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специализация «Управление безопасностью телекоммуникационных систем и сетей», одобренного Ученым советом университета протокол №9 «27» 02 20 23 г., на заседании кафедры ИБ протокол №10 от 30.08.2023.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа практики пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специализация «Управление безопасностью телекоммуникационных систем и сетей», одобренного Ученым советом университета протокол №9 «27» 03 2024 г., на заседании кафедры *информационной безопасности*, протокол № 12 от «24» 06 2024 г.

Зав. кафедрой _____ Марухленко А.Л.

Рабочая программа практики пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специализация «Управление безопасностью телекоммуникационных систем и сетей», одобренного Ученым советом университета протокол №9 «31» 03 2025 г., на заседании кафедры *информационной безопасности*, протокол № 12 от «24» 06 2025 г.

Зав. кафедрой _____ Шаповалов М.О.

Рабочая программа практики пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специализация «Управление безопасностью телекоммуникационных систем и сетей», одобренного Ученым советом университета протокол №___ «__»_____20___г., на заседании кафедры *информационной безопасности*, протокол № ___ от «___»_____202__ г.

Зав. кафедрой _____

Рабочая программа практики пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специализация «Управление безопасностью телекоммуникационных систем и сетей», одобренного Ученым советом университета протокол №___ «__»_____20___г., на заседании кафедры *информационной безопасности*, протокол № ___ от «___»_____202__ г.

Зав. кафедрой _____

Рабочая программа практики пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специализация «Управление безопасностью телекоммуникационных систем и сетей», одобренного Ученым советом университета протокол №___ «__»_____20___г., на заседании кафедры *информационной безопасности*, протокол № ___ от «___»_____202__ г.

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 информационной безопасности в условиях реального производства.

1.2. Задачи практики

1. Формирование профессиональных компетенций, установленных ФГОС ВО и закрепленных учебным планом за производственной преддипломной практикой.
2. Освоение современных технологий и технических средст, 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 – преддипломная.

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

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

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

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

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

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

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

Таблица 2 – Результаты обучения по практике

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за практикой)		*Код и наименование индикатора достижения компетенции, закрепленного за практикой*	*Планируемые результаты обучения по практике, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
ПК-1	Способен проводить теоретические и экспериментальные исследования защищённости телекоммуникационных систем и сетей	ПК-1.1 Формулирует тезисы из анализируемой научно-технической литературы	***Знать:*** основные тенденции в развитии современного информационного обществ и проблемы информационной безопасности. ***Уметь:*** использовать разнообразные источники информации для получения новых знаний по проблемам информационной безопасности. ***Владеть:*** Навыками подготовки аналитических отчётов по актуальным проблемам информационной безопасности.
		ПК-1.2 Разрабатывает формальные модели обработки и передачи данных в телекоммуникационных системах	***Знать:*** принципы обработки и передачи данных в ТКС, номенклатуру средств обработки данных ***Уметь:*** на основе имеющихся сведений о

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за практикой)		*Код и наименование индикатора достижения компетенции, закрепленного за практикой*	*Планируемые результаты обучения по практике, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			ТКС формулировать абстрактные модели циркуляции данных в них ***Владеть (****или* ***Иметь опыт деятельности):*** формализации и математической интерпретации процессов обработки и передачи данных в ТКС
		ПК-1.3 Формулирует целевые критерии для оценивания эффективности исследуемых систем	***Знать:*** основные источники информации по профессиональной тематике. ***Уметь:*** сопоставлять известные методы и средства обеспечения информационной безопасности потребностям заказчика и условиям конкретного объекта. ***Владеть:*** навыками решения задач комплексного обеспечения информационной безопасности телекоммуникационных систем.
		ПК-1.4 Проводит экспериментальные и теоретические исследования защищённости телекоммуникационных систем и сетей	***Знать:*** Принципы организации исследований и процессов телекоммуникационных систем. ***Уметь:*** Формулировать задачи, планировать и проводить исследования в сфере информационной

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за практикой)		*Код и наименование индикатора достижения компетенции, закрепленного за практикой*	*Планируемые результаты обучения по практике, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			безопасности. ***Владеть:*** Навыками планирования и проведения исследования объектов, явлений и процессов телекоммуникационных систем.
ПК-6	Способен управлять работами по обеспечению информационной безопасности	ПК-6.1 Определяет перечень информации, подлежащей защите	***Знать:*** Принципы организации телекоммуникационных систем и их уязвимости. ***Уметь:*** Формулировать технические требования к телекоммуникационным системам и мерам по предотвращению уязвимостей. ***Владеть:*** навыками создания моделей угроз и моделей злоумышленника для телекоммуникационных систем и устройств.
		ПК-6.2 Определяет требуемый уровень защищённости информации, циркулирующей в телекоммуникационной системе	***Знать:*** законы, технологии, правила, приемы обработки исследования уровня защищенности объектов информатизации. ***Уметь:*** подготовить развернутый отчет по результатам обследования объекта. ***Владеть:*** навыками подготовки аттестационных документов на предмет соответствия объекта

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за практикой)		*Код и наименование индикатора достижения компетенции, закрепленного за практикой*	*Планируемые результаты обучения по практике, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			требованиям по информационной безопасности.
		ПК-6.3 Определяет меры для защиты в информации в телекоммуникационных системах и сетях	***Знать:*** Инструментальные средства обеспечения защиты информации телекоммуникационных систем. ***Уметь:*** Осуществлять рациональный выбор средств обеспечения информационной безопасности телекоммуникационных систем. ***Владеть:*** Навыками эксплуатации телекоммуникационных приборов и средств защиты информации.
ПК-7	Способен документально обеспечивать процесса защиты информации в телекоммуникационных системах и сетях	ПК-7.1 Разрабатывает технические задания на модернизацию систем защиты информации	***Знать:*** структуру и содержание технических заданий на проведение работ по обеспечению информационной безопасности ***Уметь:*** формулировать задачи и уели модернизации системы обеспечения информационной безопасности ***Владеть (***или ***Иметь опыт деятельности):*** формулирования заданий для обеспечения информационной безопасности

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за практикой)		*Код и наименование индикатора достижения компетенции, закрепленного за практикой*	*Планируемые результаты обучения по практике, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
		ПК-7.2 Формирует документы для обоснования разработки и модернизации систем защиты информации	***Знать:*** правила выполнения работ по обеспечению информационной безопасности ***Уметь:*** документально описывать применяемые для обеспечения безопасности ТКС технологии ***Владеть (****или* ***Иметь опыт деятельности):*** разработки и модернизации систем защиты информации
		ПК-7.3 Разрабатывает модели угроз и модели нарушителей	***Знать:*** принципы и структуру моделей угроз и моделей нарушителя ***Уметь:*** соотносить уязвимости в телекоммуникационных системах возможностям злоумышленников ***Владеть (****или* ***Иметь опыт деятельности):*** определения категорий злоумышленников исходя из характеристик телекоммуникационных систем
		ПК-7.4 Готовит проекты нормативных и методических материалов, регламентирующих выполнение работ по защите информации	***Знать:*** структуру и состав нормативных документов по обеспечению информационной безопасности ***Уметь:*** анализировать имеющиеся требования нормативных документов и формулировать положения по

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за практикой)		*Код и наименование индикатора достижения компетенции, закрепленного за практикой*	*Планируемые результаты обучения по практике, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			проведению работ по обеспечению информационной безопасности ***Владеть (****или* ***Иметь опыт деятельности):*** проведения и документального обеспечения работ по информационной безопасности
ПК-8	Способен организовать работы по выполнению требований защиты информации ограниченного доступа в телекоммуникационных системах и сетях	ПК-8.1 Управляет работой специалистов по созданию и эксплуатации средств защиты информации в телекоммуникационных системах и сетях	***Знать:*** порядок действий специалистов по созданию и эксплуатации средств защиты информации в телекоммуникационных системах и сетях ***Уметь:*** ставить задачи отдельным исполнителям при создании и эксплуатации средств защиты информации в телекоммуникационных системах и сетях ***Владеть (****или* ***Иметь опыт деятельности):*** созданияю и эксплуатации средств защиты информации в телекоммуникационных системах и сетях
		ПК-8.2 Формирует комплекс мер (принципов, правил, процедур, практических приемов, методов, средств) для защиты в телекоммуникационных системах и сетях информации ограниченного доступа	***Знать:*** перечень угроз, на нейтрализацию которых направлена та или иная мера по защите информации ***Уметь:*** объединять отдельные мероприятия по обеспечению информационной безопасности в логически структурированные

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за практикой)		*Код и наименование индикатора достижения компетенции, закрепленного за практикой*	*Планируемые результаты обучения по практике, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			последовательности ***Владеть (****или* ***Иметь опыт деятельности):*** использования отдельных технологий обеспечения информационной безопасности в ТКС
		ПК-8.3 Управляет процессом разработки моделей угроз и моделей нарушителя безопасности компьютерных систем	***Знать:*** административный регламент проведения работ по обеспечению информационной безопасности ***Уметь:*** принимать управленческие решения при проведении работ по обеспечению информационной безопасности ***Владеть (****или* ***Иметь опыт деятельности):*** разработки моделей угроз и моделей нарушителя безопасности компьютерных систем
		ПК-8.4 Разрабатывает организационно-распорядительные документы, регламентирующие порядок эксплуатации телекоммуникационных систем и сетей	***Знать:*** основные этапы жизненного цикла ТКС и регламентные мероприятия на каждом из них ***Уметь:*** выполнять отдельных действий по обеспечению информационной безопасности телекоммуникационных систем ***Владеть (****или* ***Иметь опыт деятельности):*** систематизации отдельных действий по обеспечению

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за практикой)		*Код и наименование индикатора достижения компетенции, закрепленного за практикой*	*Планируемые результаты обучения по практике, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			информационной безопасности телекоммуникационных систем
		ПК 8.5 Определяет действия сотрудников при проведении мероприятий по информационной безопасности	***Знать:*** правовые нормы действующего законодательства, регулирующие отношения в различных сферах жизнедеятельности; ***Уметь:*** определять направления актуализации системы защиты информации в соответствии с текущими деловыми потребностями фирмы и выявленным уровнем уязвимости защищаемой информации; ***Владеть (****или* ***Иметь опыт деятельности):*** применения нормативных правовых документов в своей деятельности; - навыками работы с информацией из различных источников;
ПК-9	Способен эксплуатировать телекоммуникационные системы в защищённом исполнении	ПК-9.1 Выявляет сбои и отказы устройств и программ	***Знать:*** основные признаки возникновения сбоев и отказов при эксплуатации ТКС ***Уметь:*** в процессе эксплуатации фиксировать режимы работы ТКС, отличные от штатных ***Владеть (****или* ***Иметь опыт деятельности):*** обнаружения сбоев и

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за практикой)		*Код и наименование индикатора достижения компетенции, закрепленного за практикой*	*Планируемые результаты обучения по практике, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			отказов реальных ТКС
		ПК-9.2 Восстанавливает работоспособность систем после сбоев и отказов устройств и программ	***Знать:*** знать номенклатуру регламентных работ по восстановлению работоспособности устройств и программ ***Уметь:*** выполнять регламентные работы по восстановлению работоспособности устройств и программ ***Владеть (****или* ***Иметь опыт деятельности):*** эксплуатации программного и аппартного обеспечения ТКС в различных режимах работы
		ПК-9.3 Формулирует перечень действий для восстановления последствий сбоев и отказов	***Знать:*** назначение и классификацию программно-аппаратных средств ТКС; особенности функционирования ТКС; классификацию программных и аппаратных средств анализа защищённости ТКС, систем обнаружения сетевых атак, антивирусного ПО; технические характеристики и правила эксплуатации средств восстановления последствий сбоев и отказов. ***Уметь:*** проводить мониторинг безопасности АС; обнаруживать уязвимые места в

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за практикой)		*Код и наименование индикатора достижения компетенции, закрепленного за практикой*	*Планируемые результаты обучения по практике, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			функционировании ПО и оборудования ТКС; провести настройку ПО и оборудования ТКС. ***Владеть:*** навыками настройки программных и аппаратных средств анализа защищённости ТКС, систем обнаружения сетевых атак, антивирусного ПО.
		ПК-9.4 Регистрирует сообщения об ошибках в сетевых устройствах и операционных системах	***Знать:*** основные признаки возникновения ошибок в сетевых устройствах и операционных системах ***Уметь:*** в процессе эксплуатации фиксировать режимы работы сетевых устройств и операционных систем, отличные от штатных ***Владеть (****или* ***Иметь опыт деятельности):*** навыками обнаружения сбоев и отказов реальных сетевых устройств и операционных систем
		ПК-9.5 Формирует отчёты по результатам работ системы мониторинга	***Знать:*** структуру и содержание журналов аудита информационной безопасности ***Уметь:*** использовать технические средства ведения журналов аудита информационной безопасности ***Владеть (****или* ***Иметь***

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за практикой)		*Код и наименование индикатора достижения компетенции, закрепленного за практикой*	*Планируемые результаты обучения по практике, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			опыт деятельности): навыками анализа журналов аудита информационной безопасности
ПК-10	Способен эксплуатировать средства обеспечения информационной безопасности для реализации политик безопасности	ПК-10.1 Проверяет корректность работы программных компонент телекоммуникационной системы	***Знать:*** основные признаки возникновения ошибок в программных компонентах телекоммуникационной системы ***Уметь:*** в процессе эксплуатации фиксировать режимы работы программных компонент телекоммуникационной системы, отличные от штатных ***Владеть (****или* ***Иметь опыт деятельности):*** навыками обнаружения сбоев и отказов в программных компонентах телекоммуникационной системы
		ПК-10.2 Определяет соответствие текущего функционала системы требованиям профилей защиты	***Знать:*** Профили защиты инструментальные средства обеспечения защиты информации телекоммуникационных систем. ***Уметь:*** Осуществлять рациональный выбор средств реализации профилей защиты. ***Владеть:*** Навыками работы с профилями защиты.

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за практикой)		*Код и наименование индикатора достижения компетенции, закрепленного за практикой*	*Планируемые результаты обучения по практике, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
		ПК-10.3 Формирует систематизированные политики информационной безопасности	***Знать:*** основные этапы жизненного цикла ТКС и регламентные мероприятия на каждом из них ***Уметь:*** ***Владеть (****или* ***Иметь опыт деятельности):*** систематизации отдельных действие по обеспечению информационной безопасности телекоммуникационных систем
		ПК-10.4 Разрабатывает профили заданий по безопасности для оборудования телекоммуникационных систем в защищённом исполнении	***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
ПК-11	Способен управлять жизненным циклом подсистем обеспечения информационной безопасности	ПК-11.1 Определяет действия по обеспечению информационной безопасности на различных этапах жизненного цикла телекоммуникационной	***Знать:*** особенности различных этапов жизненного цикла ТКС ***Уметь:*** исходя их имеющегося перечня угроз реализовывать технологии обеспечения информационной

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за практикой)		*Код и наименование индикатора достижения компетенции, закрепленного за практикой*	*Планируемые результаты обучения по практике, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
		системы	безопасности ***Владеть (****или* ***Иметь опыт деятельности):*** эксплуатации ТКС на различных этапах жизненного цикла
		ПК-11.2 Выбирает перечень реализуемых телекоммуникационной системой технологий для удовлетворения требований по информационной безопасности	***Знать:*** перечень реализуемых телекоммуникационной системой технологий для удовлетворения требований по информационной безопасности ***Уметь:*** **соотносить** технологии информационной безопасности существующим в ТКС уязвимостям ***Владеть (****или* ***Иметь опыт деятельности):*** **реализации** технологий информационной безопасности
		ПК-11.3 Оценивает результат применения штатных средств обеспечения информационной безопасности	***Знать:*** критерии результативности применения штатных средств обеспечения информационной безопасности ***Уметь:*** формулировать количественные критерии результативности применения штатных средств обеспечения информационной безопасности ***Владеть (****или* ***Иметь опыт деятельности):*** навыками оценки результативности применения штатных средств обеспечения

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за практикой)		*Код и наименование индикатора достижения компетенции, закрепленного за практикой*	*Планируемые результаты обучения по практике, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			информационной безопасности
		ПК-11.4 Формулирует предложения по совершенствованию подсистем обеспечения информационной безопасности	***Знать:*** меры и технологии, направленные на повышение защищённости процессов обработки информации в ТКС ***Уметь:*** **определять** меры и технологии, направленные на повышение защищённости процессов обработки информации в конкретной ТКС ***Владеть (****или* ***Иметь опыт деятельности):*** обеспечения процесса защиты информации в ТКС

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, – 9 зачетных единиц, продолжительность – 6 недель (324 часа).

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 6 часов, работа обучающегося в иных формах – 318 часов.

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

Таблица 4 – Этапы и содержание практики

№ п/п	Этапы практики	Содержание практики	Трудоемкость (час)
1	Подготовительный этап	Решение организационных вопросов: 1) распределение обучающихся по местам практики; 2) знакомство с целью, задачами, программой, порядком прохождения практики; 3) получение заданий от руководителя практики от университета; 4) информация о требованиях к отчетным документам по практике; 5) первичный инструктаж по технике безопасности.	2
2	Основной этап	Работа обучающихся в профильной организации	186
2.1	Знакомство с профильной организацией	Знакомство с профильной организацией, руководителем практики от организации, рабочим местом и должностной инструкцией.	2
		Инструктаж по технике безопасности на рабочем месте.	5

		Знакомство с содержанием деятельности профильной организации по обеспечению информационной безопасности и проводимыми в нем мероприятиями.	3
		Изучение нормативных правовых актов профильной организации по обеспечению информационной безопасности (политика безопасности профильной организации, положения, приказы, инструкции, должностные обязанности, памятки и др.).	
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 проведения мониторинга безопасности ТКС. Создание плана работы коллектива из 3 – 4 человек, реализующего политику безопасности в ТКС	90.
		Самостоятельная обработка и систематизация полученных данных с помощью профессиональных программных комплексов и информационных технологий. *Организация работы 2-3 человек и руководство их работой в процессе обработки и систематизации полученных данных.* Представление результатов мониторинга руководителю практики от организации	
		Самостоятельное проведение	

		анализа результатов проведенного мониторинга информационной безопасности. Организация работы 2-3 человек и руководство их работой в процессе работ по обеспечению информационной безопасности. 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 повышению уровня информационной безопасности предприятия.* Представление своих рекомендаций руководителю практики от организации.	
		Самостоятельное составление краткосрочного плана работ по обеспечению безопасности организации, эксплуатирующей ТКС. *Организация работы 2-3 человек и руководство их работой в процессе составления краткосрочного и долгосрочного прогнозов.* Представление своего прогноза с обоснованием руководителю практики от организации.	
3	Заключительный этап	Оформление дневника практики.	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 мониторинга.

– Оценка рисков информационной безопасности ТКС.

– Рекомендации по повышению уровня информационной безопасности предприятия.

– Краткосрочный и долгосрочный прогноз развития ситуации.

5) Заключение. Выводы о достижении цели и выполнении задач практики.
6) Список использованной литературы и источников.
7) Приложения (иллюстрации, таблицы, карты и т.п.).

Отчет должен быть оформлен в соответствии с:

– ГОСТ Р 7.0.12-2011 Библиографическая запись. Сокращение слов и словосочетаний на русском языке. Общие требования и правила.

– ГОСТ 2.316-2008 Единая система конструкторской документации. Правила нанесения надписей, технических требований и таблиц на графических документах. Общие положения;

– ГОСТ 7.32-2001 Отчет о научно-исследовательской работе. Структура и правила оформления;

– ГОСТ 2.105-95 ЕСКД. Общие требования к текстовым документам;

– ГОСТ 7.1-2003 Система стандартов по информации, библиотечному и издательскому делу. Общие требования и правила составления;

– ГОСТ 2.301-68 Единая система конструкторской документации. Форматы;

– ГОСТ 7.82-2001 Библиографическая запись. Библиографическое описание электронных ресурсов. Общие требования и правила составления;

– ГОСТ 7.9-95 (ИСО 214-76). Система стандартов по информации, библиотечному и издательскому делу. Реферат и аннотация. Общие требования.

– СТУ 04.02.030-2015 «Курсовые работы (проекты). Выпускные квалификационные работы. Общие требования к структуре и оформлению».

6 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по практике

6.1 Перечень компетенций с указанием этапов их формирования в процессе освоения основной профессиональной образовательной программы

Таблица 6.1 – Этапы формирования компетенций

Код и наименование компетенции	Этапы* формирования компетенций и дисциплины (модули), практики, НИР, при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
ПК-1	Квантовая и оптическая электроника Физические основы оптических систем связи	Производственная преддипломная практика	
ПК-6	Комплексная защита объектов информатизации	Производственная преддипломная практика	
ПК-7	Порядок проведения аттестации объектов информатизации	Производственная преддипломная практика	
ПК-8	Организация и управление службой защиты информации Система сертификации и лицензирования деятельности по защите информации	Порядок проведения аттестации объектов информатизации	Производственная преддипломная практика
ПК-9	Комплексная защита объектов информатизации	Производственная преддипломная практика	
ПК-10	Информационная безопасность телекоммуникационных	Инфокоммуникационные системы навигации и диспетчеризации и их	Производственная преддипломная практика

	систем	защита Безопасность средств мониторинга территорий и объектов	
ПК-11	Комплексная защита объектов информатизации	Производственная преддипломная 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 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
ПК-1/ завершающий	ПК-1.1 Формулирует тезисы из анализируемой научно-технической литературы	**Знать:** Фрагментарные знания о тенденциях в развитии современного информационного обществ и проблемы информационной безопасности. **Уметь:** Сформированное умение использовать разнообразные источники информации для получения новых знаний по проблемам информационной безопасности. **Владеть (**или **Иметь опыт деятельности):**	**Знать:** Сформированные, но содержащие отдельные пробелы знания о тенденциях в развитии современного информационного обществ и проблемы информационной безопасности. **Уметь:** Сформированное умение использовать разнообразные источники информации для получения новых знаний по проблемам информационной безопасности. **Владеть (**или	***Знать:*** Глубокие знания о тенденциях в развитии современного информационного обществ и проблемы информационной безопасности. ***Уметь:*** Уверенно и на высоком уровне использовать разнообразные источники информации для получения новых знаний по проблемам информационной безопасности. ***Владеть:*** Уверенно владеет навыками подготовки

1	2	3	4	5
		Владеет базовыми навыками подготовки аналитических отчётов по актуальным проблемам информационной безопасности.	**Иметь опыт деятельности):** Владеет основными навыками подготовки аналитических отчётов по актуальным проблемам информационной безопасности.	аналитических отчётов по актуальным проблемам информационной безопасности.
	ПК-1.2 Разрабатывает формальные модели обработки и передачи данных в телекоммуникационных системах	**Знать:** Фрагментарные знания о принципах обработки и передачи данных в ТКС, номенклатуру средств обработки данных ***Уметь:*** Сформированное умение на основе имеющихся сведений о ТКС формулировать абстрактные модели циркуляции данных в них ***Владеть (****или* ***Иметь опыт деятельности):*** Владеет базовыми навыками формализации и математической интерпретации процессов обработки и передачи данных в ТКС	**Знать:** Сформированные, но содержащие отдельные пробелы знания о принципах обработки и передачи данных в ТКС, номенклатуру средств обработки данных ***Уметь:*** Сформированное умение на основе имеющихся сведений о ТКС формулировать абстрактные модели циркуляции данных в них ***Владеть (****или* ***Иметь опыт деятельности):*** Владеет основными навыками формализации и математической интерпретации процессов обработки и передачи данных в ТКС	***Знать:*** Глубокие знания о принципах обработки и передачи данных в ТКС, номенклатуру средств обработки данных ***Уметь:*** Уверенно и на высоком уровне на основе имеющихся сведений о ТКС формулировать абстрактные модели циркуляции данных в них ***Владеть (****или* ***Иметь опыт деятельности):*** Уверенно владеет навыками формализации и математической интерпретации процессов обработки и передачи данных в ТКС
	ПК-1.3 Формулирует целевые критерии для оценивания эффективно	***Знать:*** основные источники информации по профессиональной тематике. ***Уметь:*** сопоставлять	***Знать:*** Требующиеся для выполнения профессиональных действий источники информации по профессиональной	***Знать:*** Широкий спектр источников и информации по профессиональной тематике. ***Уметь:*** сопоставлять

1	2	3	4	5
	сти исследуемых систем	основные методы и средства обеспечения информационной безопасности потребностям заказчика и условиям объекта невысокой сложности. ***Владеть:*** навыками решения базовых задач комплексного обеспечения информационной безопасности телекоммуникационных систем.	тематике. ***Уметь:*** сопоставлять известные методы и средства обеспечения информационной безопасности типовым потребностям заказчика и условиям типового объекта. ***Владеть:*** навыками решения стандартных задач комплексного обеспечения информационной безопасности телекоммуникационных систем.	нетиповые методы и средства обеспечения информационной безопасности потребностям заказчика и условиям конкретного объекта. ***Владеть:*** навыками решения нестандартных задач комплексного обеспечения информационной безопасности телекоммуникационных систем.
	ПК-1.4 Проводит экспериментальные и теоретические исследования защищённости телекоммуникационных систем и сетей.	***Знать:*** Принципы организации элементов процессов телекоммуникационных систем. ***Уметь:*** реализовывать задачи, планировать и проводить исследования в сфере информационной безопасности. ***Владеть:*** владеет навыками проведения исследования объектов под непосредственным руководством.	***Знать:*** Принципы организации исследований и процессов телекоммуникационных систем. ***Уметь:*** Формулировать типовые задачи, планировать и проводить исследования в сфере информационной безопасности. ***Владеть:*** владеет навыками планирования и проведения исследования объектов, явлений и процессов телекоммуникационных систем.	***Знать:*** Принципы организации исследований нестандартных процессов телекоммуникационных систем. ***Уметь:*** Формулировать и прорабатывать задачи, планировать и проводить исследования в сфере информационной безопасности. ***Владеть:*** Уверенно владеет навыками планирования и проведения исследования объектов, явлений и процессов телекоммуникационных систем.
ПК-6/	ПК-6.1	***Знать:***	***Знать:***	***Знать:***

1	2	3	4	5
завершающий	Определяет перечень информации, подлежащей защите	Основные уязвимости телекоммуникационных систем. ***Уметь:*** Формулировать отдельные требования к телекоммуникационным системам и мерам по предотвращению уязвимостей. ***Владеть:*** навыками создания примитивных моделей угроз и моделей злоумышленника для телекоммуникационных систем и устройств.	Принципы организации телекоммуникационных систем и их основные уязвимости. ***Уметь:*** Формулировать технические требования к телекоммуникационным системам и мерам по предотвращению уязвимостей. ***Владеть:*** навыками создания стандартных моделей угроз и моделей злоумышленника для телекоммуникационных систем и устройств.	Принципы организации телекоммуникационных систем и их уязвимости, в том числе нетиповые. ***Уметь:*** Прорабатывать и детализировать технические требования к телекоммуникационным системам и мерам по предотвращению уязвимостей. ***Владеть:*** навыками создания сложных и нетиповых моделей угроз и моделей злоумышленника для телекоммуникационных систем и устройств.
	ПК-6.2 Определяет требуемый уровень защищённости информации, циркулирующей в телекоммуникационной системе	***Знать:*** Фрагменты и отдельные законов, технологий, правил, приемов обработки исследования уровня защищенности объектов информатизации. ***Уметь:*** подготовить отдельные части отчета по результатам обследования объекта. ***Владеть:*** навыками подготовки отдельных аттестационных документов на предмет	***Знать:*** Основные законы, технологии, правила, приемы обработки исследования уровня защищенности объектов информатизации. ***Уметь:*** подготовить отчет по результатам обследования объекта. ***Владеть:*** навыками подготовки аттестационных документов на предмет соответствия объекта требованиям по информационной	***Знать:*** Совокупность законов, технологий, правил, приемов обработки исследования уровня защищенности объектов информатизации. ***Уметь:*** подготовить развернутый отчет по результатам обследования объекта. ***Владеть:*** уверенными навыками подготовки аттестационных документов на предмет соответствия

1	2	3	4	5
		соответствия объекта требованиям по информационной безопасности.	безопасности.	объекта требованиям по информационной безопасности.
	ПК-6.3 Определяет меры для защиты в информации в телекоммуникационных системах и сетях	***Знать:*** Назначение инструментальных средств обеспечения защиты информации телекоммуникационных систем. ***Уметь:*** Выделять требуемые характеристики средств обеспечения информационной безопасности телекоммуникационных систем. ***Владеть:*** Базовыми навыками эксплуатации телекоммуникационных приборов и средств защиты информации.	***Знать:*** Инструментальные средства обеспечения защиты информации телекоммуникационных систем. ***Уметь:*** Осуществлять выбор средств обеспечения информационной безопасности телекоммуникационных систем. ***Владеть:*** Навыками эксплуатации телекоммуникационных приборов и средств защиты информации.	***Знать:*** Полный спектр инструментальных средств обеспечения защиты информации телекоммуникационных систем. ***Уметь:*** Осуществлять рациональный выбор средств обеспечения информационной безопасности телекоммуникационных систем. ***Владеть:*** Уверенными навыками эксплуатации телекоммуникационных приборов и средств защиты информации.
ПК-7/ завершающий	ПК-7.1 Разрабатывает технические задания на модернизацию систем защиты информации	***Знать:*** структуру и содержание технических заданий на проведение отдельных этапов работ по обеспечению информационной безопасности ***Уметь:*** формулировать последовательности задач по модернизации системы обеспечения	***Знать:*** структуру и содержание технических заданий на проведение основных этапов работ по обеспечению информационной безопасности ***Уметь:*** формулировать задачи и цели модернизации системы обеспечения информационной	***Знать:*** структуру и содержание технических заданий на проведение работ по обеспечению информационной безопасности ***Уметь:*** формулировать задачи и цели модернизации системы обеспечения информационной безопасности и критерии их

1	2	3	4	5
		информационной безопасности ***Владеть (****или* ***Иметь опыт деятельности):*** формулирования этапов работ по обеспечению информационной безопасности	безопасности ***Владеть (****или* ***Иметь опыт деятельности):*** формулирования заданий для обеспечения информационной безопасности	достижения ***Владеть (****или* ***Иметь опыт деятельности):*** формулирования проработанных заданий для обеспечения информационной безопасности
	ПК-7.2 Формирует документы для обоснования разработки и модернизации систем защиты информации	***Знать:*** номенклатуру правил выполнения работ по обеспечению информационной безопасности ***Уметь:*** с недостатками документально описывать применяемые для обеспечения безопасности ТКС технологии ***Владеть (****или* ***Иметь опыт деятельности):*** проведения работ по разработке и модернизации систем защиты информации	***Знать:*** основные правила выполнения работ по обеспечению информационной безопасности ***Уметь:*** документально описывать основные применяемые для обеспечения безопасности ТКС технологии ***Владеть (****или* ***Иметь опыт деятельности):*** разработки и модернизации систем защиты информации	***Знать:*** правила, регламенты и порядок выполнения работ по обеспечению информационной безопасности ***Уметь:*** документально и в полном объёме описывать применяемые для обеспечения безопасности ТКС технологии ***Владеть (****или* ***Иметь опыт деятельности):*** разработки и модернизации систем защиты информации для достижения целевых показателей функционирования
	ПК-7.3 Разрабатывает модели угроз и модели нарушителей	***Знать:*** структуру моделей угроз и моделей нарушителя ***Уметь:*** формулировать возможности злоумышленников ***Владеть (****или* ***Иметь опыт деятельности):*** сопоставления категорий злоумышленников характеристикам	***Знать:*** принципы и структуру моделей угроз и моделей нарушителя ***Уметь:*** соотносить уязвимости в телекоммуникационных системах возможностям злоумышленников ***Владеть (****или* ***Иметь опыт деятельности):*** определения категорий	***Знать:*** фундаментальные принципы и структуру моделей угроз и моделей нарушителя ***Уметь:*** соотносить уязвимости в сложных и нетиповых телекоммуникационных системах возможностям злоумышленников ***Владеть (****или*

1	2	3	4	5
		телекоммуникационных систем	злоумышленников исходя из характеристик телекоммуникационных систем	***Иметь опыт деятельности):*** формирования оригинальных методик определения категорий злоумышленников исходя из характеристик телекоммуникационных систем
	ПК-7.4 Готовит проекты нормативных и методических материалов, регламентирующих выполнение работ по защите информации	***Знать:*** номенклатуру нормативных документов по обеспечению информационной безопасности ***Уметь:*** сопоставлять этапы работ по обеспечению информационной безопасности целям организации ***Владеть (****или* ***Иметь опыт деятельности):*** проведения работ по информационной безопасности	***Знать:*** структуру и состав основных нормативных документов по обеспечению информационной безопасности ***Уметь:*** определять этапы работ по обеспечению информационной безопасности ***Владеть (****или* ***Иметь опыт деятельности):*** проведения и документального обеспечения работ по информационной безопасности	***Знать:*** полную структуру и состав нормативных документов по обеспечению информационной безопасности ***Уметь:*** анализировать имеющиеся требования нормативных документов и формулировать положения по проведению работ по обеспечению информационной безопасности ***Владеть (****или* ***Иметь опыт деятельности):*** проведения и точного документального обеспечения работ по информационной безопасности
ПК-8/ завершающий	ПК-8.1 Управляет работой специалистов по созданию и эксплуатации средств защиты информаци	***Знать:*** порядок действий специалистов по эксплуатации средств защиты информации в телекоммуникационных системах и сетях ***Уметь:*** ставить	***Знать:*** порядок действий специалистов по созданию и эксплуатации средств защиты информации в телекоммуникационных системах и сетях	***Знать:*** методику определения порядка действий специалистов по созданию и эксплуатации средств защиты информации в телекоммуникационных системах и

1	2	3	4	5
	и в телекоммуникационных системах и сетях	задачи отдельным исполнителям и эксплуатации средств защиты информации в телекоммуникационных системах и сетях ***Владеть (****или* ***Иметь опыт деятельности):*** эксплуатации средств защиты информации в телекоммуникационных системах и сетях	***Уметь:*** ставить задачи отдельным исполнителям при создании и эксплуатации средств защиты информации в телекоммуникационных системах и сетях ***Владеть (****или* ***Иметь опыт деятельности):*** созданию и эксплуатации средств защиты информации в телекоммуникационных системах и сетях	сетях ***Уметь:*** ставить задачи всем исполнителям при создании и эксплуатации средств защиты информации в телекоммуникационных системах и сетях ***Владеть (****или* ***Иметь опыт деятельности):*** создания и эксплуатации сложных средств защиты информации в телекоммуникационных системах и сетях
	ПК-8.2 Формирует комплекс мер (принципов, правил, процедур, практических приемов, методов, средств) для защиты в телекоммуникационных системах и сетях информации ограниченного доступа	***Знать:*** перечень угроз, на нейтрализацию которых направлены отдельные меры по защите информации ***Уметь:*** проводить отдельные мероприятия по обеспечению информационной безопасности в логически структурированные последовательности ***Владеть (****или* ***Иметь опыт деятельности):*** использования отдельных технологий обеспечения информационной безопасности в ТКС	***Знать:*** перечень угроз, на нейтрализацию которых направлена та или иная мера по защите информации ***Уметь:*** последовательно проводить отдельные мероприятия по обеспечению информационной безопасности в логически структурированные последовательности ***Владеть (****или* ***Иметь опыт деятельности):*** использования типовых технологий обеспечения информационной безопасности в	***Знать:*** методики определения угроз, на нейтрализацию которых направлена та или иная мера по защите информации ***Уметь:*** объединять отдельные мероприятия по обеспечению информационной безопасности в логически структурированные последовательности ***Владеть (****или* ***Иметь опыт деятельности):*** использования разнообразных технологий обеспечения информационной безопасности в ТКС

1	2	3	4	5
			ТКС	
	ПК-8.3 Управляет процессом разработки моделей угроз и моделей нарушителя безопасности компьютерных систем	***Знать:*** административный регламент проведения работ по обеспечению информационной безопасности ***Уметь:*** при поддержке принимать управленческие решения при проведении работ по обеспечению информационной безопасности ***Владеть (****или* ***Иметь опыт деятельности):*** разработки элементов моделей угроз и моделей нарушителя безопасности компьютерных систем	***Знать:*** административный регламент проведения работ по обеспечению информационной безопасности ***Уметь:*** принимать управленческие решения при проведении работ по обеспечению информационной безопасности ***Владеть (****или* ***Иметь опыт деятельности):*** разработки моделей угроз и моделей нарушителя безопасности для типовых компьютерных систем	***Знать:*** правила и административный регламент проведения работ по обеспечению информационной безопасности ***Уметь:*** принимать и обосновывать управленческие решения при проведении работ по обеспечению информационной безопасности ***Владеть (****или* ***Иметь опыт деятельности):*** разработки оригинальных моделей угроз и моделей нарушителя безопасности компьютерных систем
	ПК-8.4 Разрабатывает организационно-распорядительные документы, регламентирующие порядок эксплуатации телекоммуникационных систем и сетей	***Знать:*** номенклатуру этапов жизненного цикла ТКС и регламентные мероприятия на каждом из них ***Уметь:*** выполнять отдельные действия по обеспечению информационной безопасности телекоммуникационных систем ***Владеть (****или* ***Иметь опыт деятельности):*** систематизации отдельных действий по обеспечению информационной безопасности	***Знать:*** основные этапы жизненного цикла ТКС и регламентные мероприятия на каждом из них ***Уметь:*** выполнять небольшие последовательности отдельных действий по обеспечению информационной безопасности телекоммуникационных систем ***Владеть (****или* ***Иметь опыт деятельности):*** систематизации последовательности действий по обеспечению информационной	***Знать:*** все возможные этапы жизненного цикла ТКС и регламентные мероприятия на каждом из них ***Уметь:*** выполнять связанные последовательности действий по обеспечению информационной безопасности телекоммуникационных систем ***Владеть (****или* ***Иметь опыт деятельности):*** систематизации сложных последовательностей действий по обеспечению

1	2	3	4	5
		телекоммуникационных систем	безопасности телекоммуникационных систем	информационной безопасности телекоммуникационных систем
	ПК 8.5 Определяет действия сотрудников при проведении мероприятий по информационной безопасности	**Знать**: Организацию судебных, правоприменительных и правоохранительных органов **Уметь**: определять перечень действий для проведения анализа ИБ **Владеть (или Иметь опыт деятельности):** Навыками работы с нормативно-правовыми документами	**Знать**: правовые нормы действующего законодательства, регулирующие отношения в различных сферах жизнедеятельности. **Уметь**: работать с нормативными документами регуляторов в области информационной безопасности **Владеть (или Иметь опыт деятельности):** работой с методической литературой и вырабатывать управленческие решения в области информационной безопасности;	**Знать**: основные положения и нормы конституционного, гражданского, семейного, трудового, административного и уголовного права. **Уметь**: определять актуальные вопросы защиты информации в соответствии с уровнем уязвимости **Владеть (или Иметь опыт деятельности):** Навыками применения нормативных правовых документов в конкретных практических ситуациях
ПК-9/ завершающий	ПК-9.1 Выявляет сбои и отказы устройств и программ	***Знать:*** отдельные признаки возникновения сбоев и отказов при эксплуатации ТКС ***Уметь:*** под руководством в процессе эксплуатации фиксировать режимы работы ТКС, отличные от штатных ***Владеть (или Иметь опыт деятельности):*** обнаружения части сбоев и отказов реальных ТКС	***Знать:*** основные признаки возникновения сбоев и отказов при эксплуатации ТКС ***Уметь:*** в процессе эксплуатации фиксировать режимы работы ТКС, отличные от штатных ***Владеть (или Иметь опыт деятельности):*** обнаружения сбоев и отказов типовых ТКС	***Знать:*** различные, в том числе нетиповые признаки возникновения сбоев и отказов при эксплуатации ТКС ***Уметь:*** в процессе эксплуатации выявлять и фиксировать режимы работы ТКС, отличные от штатных ***Владеть (или Иметь опыт деятельности):*** обнаружения сбоев и отказов сложных ТКС

1	2	3	4	5
	ПК-9.2 Восстанавливает работоспособность систем после сбоев и отказов устройств и программ	***Знать:*** знать номенклатуру регламентных работ по восстановлению работоспособности устройств и программ ***Уметь:*** выполнять регламентные работы по восстановлению работоспособности устройств и программ ***Владеть (****или* ***Иметь опыт деятельности):*** эксплуатации отдельных элементов программного и аппаратного обеспечения ТКС	***Знать:*** порядок проведения регламентных работ по восстановлению работоспособности устройств и программ ***Уметь:*** оперативно выполнять регламентные работы по восстановлению работоспособности устройств и программ ***Владеть (****или* ***Иметь опыт деятельности):*** эксплуатации программного и аппаратного обеспечения ТКС	***Знать:*** знать цели и задачи регламентных работ по восстановлению работоспособности устройств и программ ***Уметь:*** выполнять точно и оперативно требуемые работы по восстановлению работоспособности устройств и программ ***Владеть (****или* ***Иметь опыт деятельности):*** эксплуатации программного и аппаратного обеспечения ТКС в различных режимах работы
	ПК-9.3 Формулирует перечень действий для восстановления последствий сбоев и отказов	***Знать:*** назначение и классификацию программно-аппаратных средств ТКС; технические характеристики и правила эксплуатации средств восстановления последствий сбоев и отказов. ***Уметь:*** провести настройку ПО и оборудования ТКС. ***Владеть:*** навыками настройки, антивирусного ПО.	***Знать:*** назначение и классификацию программно-аппаратных средств ТКС; особенности функционирования ТКС; систем обнаружения сетевых атак, антивирусного ПО; технические характеристики и правила эксплуатации средств восстановления последствий сбоев и отказов. ***Уметь:*** проводить мониторинг безопасности АС; провести настройку ПО и оборудования ТКС. ***Владеть:***	***Знать:*** назначение и классификацию программно-аппаратных средств ТКС; особенности функционирования ТКС; классификацию программных и аппаратных средств анализа защищённости ТКС, систем обнаружения сетевых атак, антивирусного ПО; технические характеристики и правила эксплуатации средств восстановления последствий сбоев и отказов. ***Уметь:*** проводить мониторинг

1	2	3	4	5
			навыками настройки программных и аппаратных средств анализа защищённости ТКС, антивирусного ПО.	безопасности АС; обнаруживать уязвимые места в функционировании ПО и оборудования ТКС; провести настройку ПО и оборудования ТКС. ***Владеть:*** навыками настройки программных и аппаратных средств анализа защищённости ТКС, систем обнаружения сетевых атак, антивирусного ПО.
	ПК-9.4 Регистрирует сообщения об ошибках в сетевых устройствах и операционных системах	***Знать:*** номенклатуру ошибок в сетевых устройствах и операционных системах ***Уметь:*** в процессе эксплуатации фиксировать режимы работы сетевых устройств и операционных систем, отличные от штатных ***Владеть (****или* ***Иметь опыт деятельности):*** навыками протоколирования отдельных сбоев и отказов реальных сетевых устройств и операционных систем	***Знать:*** основные признаки возникновения ошибок в сетевых устройствах и операционных системах ***Уметь:*** в процессе эксплуатации фиксировать режимы работы сетевых устройств и операционных систем, отличные от штатных ***Владеть (****или* ***Иметь опыт деятельности):*** навыками протоколирования сбоев и отказов реальных сетевых устройств и операционных систем	***Знать:*** методику выявления признаков возникновения ошибок в сетевых устройствах и операционных системах ***Уметь:*** в процессе эксплуатации обнаруживать и фиксировать режимы работы сетевых устройств и операционных систем, отличные от штатных ***Владеть (****или* ***Иметь опыт деятельности):*** навыками обнаружения и протоколирования сбоев и отказов реальных сетевых устройств и операционных систем
	ПК-9.5 Формирует отчёты по	***Знать:*** структуру журналов аудита информационной	***Знать:*** структуру и содержание журналов аудита	***Знать:*** методику формирования журналов аудита

1	2	3	4	5
	результатам работ системы мониторинга	безопасности ***Уметь:*** под руководством использовать технические средства ведения журналов аудита информационной безопасности ***Владеть (****или* ***Иметь опыт деятельности):*** навыками формирования журналов аудита информационной безопасности	информационной безопасности ***Уметь:*** использовать технические средства ведения журналов аудита информационной безопасности ***Владеть (****или* ***Иметь опыт деятельности):*** навыками работы с журналами аудита информационной безопасности	информационной безопасности ***Уметь:*** выбирать и использовать технические средства ведения журналов аудита информационной безопасности ***Владеть (****или* ***Иметь опыт деятельности):*** навыками анализа журналов аудита информационной безопасности
ПК-10/ завершающий	ПК-10.1 Проверяет корректность работы программных компонент телекоммуникационной системы	***Знать:*** номенклатуру ошибок в программных компонентах телекоммуникационной системы ***Уметь:*** в процессе эксплуатации фиксировать режимы работы в программных компонентах телекоммуникационной системы, отличные от штатных ***Владеть (****или* ***Иметь опыт деятельности):*** навыками протоколирования отдельных сбоев и отказов в программных компонентах телекоммуникационной системы	***Знать:*** основные признаки возникновения ошибок в в программных компонентах телекоммуникационной системы ***Уметь:*** в процессе эксплуатации фиксировать режимы работы в программных компонентах телекоммуникационной системы ***Владеть (****или* ***Иметь опыт деятельности):*** навыками протоколирования сбоев и отказов в программных компонентах телекоммуникационной системы	***Знать:*** методику выявления признаков возникновения ошибок в программных компонентах телекоммуникационной системы ***Уметь:*** в процессе эксплуатации обнаруживать и фиксировать режимы работы в программных компонент телекоммуникационной системы ***Владеть (****или* ***Иметь опыт деятельности):*** навыками обнаружения и протоколирования сбоев и отказов в программных компонентах телекоммуникационной системы
	ПК-10.2 Определяет соответствие текущего функционал	***Знать:*** Понятия профиля защиты инструментальные средства	***Знать:*** Профили защиты инструментальные средства обеспечения	***Знать:*** Методику формирования профилей защиты инструментальных

1	2	3	4	5
	а системы требования м профилей защиты	обеспечения защиты информации телекоммуникационных систем. ***Уметь:*** Использовать средства реализации профилей защиты. ***Владеть:*** Навыками работы с элемнтарными профилями защиты.	защиты информации телекоммуникационных систем. ***Уметь:*** Осуществлять выбор средств реализации профилей защиты. ***Владеть:*** Навыками работы с профилями защиты.	средств обеспечения защиты информации телекоммуникационных систем. ***Уметь:*** Осуществлять рациональный выбор эффективных средств реализации профилей защиты. ***Владеть:*** Навыками работы со сложными и многоуровневыми профилями защиты.
	ПК-10.3 Формирует систематизированные политики информационной безопасности	***Знать:*** отдельные этапы жизненного цикла ТКС и регламентные мероприятия на каждом из них ***Уметь:*** выполнять действия по обеспечению информационной безопасности телекоммуникационных систем ***Владеть (****или* ***Иметь опыт деятельности):*** систематизации отдельных действие по обеспечению информационной безопасности телекоммуникационных систем	***Знать:*** основные этапы жизненного цикла ТКС и регламентные мероприятия на каждом из них ***Уметь:*** выполнять последовательности действий по обеспечению информационной безопасности телекоммуникационных систем ***Владеть (****или* ***Иметь опыт деятельности):*** систематизации действие по обеспечению информационной безопасности телекоммуникационных систем	***Знать:*** все этапы жизненного цикла ТКС и регламентные мероприятия на каждом из них ***Уметь:*** выполнять связанные последовательности действий по обеспечению информационной безопасности телекоммуникационных систем ***Владеть (****или* ***Иметь опыт деятельности):*** систематизации последовательности действий по обеспечению информационной безопасности телекоммуникационных систем
	ПК-10.4 Разрабатывает профили заданий по	***Знать:*** Структуру и содержание отдельных профилей заданий	***Знать:*** Структуру и содержание профилей заданий по безопасности	***Знать:*** Методику формирования профилей заданий по безопасности

1	2	3	4	5
	безопасности для оборудования телекоммуникационных систем в защищённом исполнении	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	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	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
ПК-11/ завершающий	ПК-11.1 Определяет действия по обеспечению информационной безопасности на различных этапах жизненного цикла телекоммуникационной системы	***Знать:*** номенклатуру этапов жизненного цикла ТКС ***Уметь:*** исходя их ограниченного перечня угроз реализовывать технологии обеспечения информационной безопасности ***Владеть (****или* ***Иметь опыт деятельности):*** эксплуатации ТКС на отдельных этапах жизненного цикла	***Знать:*** характеристики различных этапов жизненного цикла ТКС ***Уметь:*** исходя их имеющегося перечня угроз реализовывать технологии обеспечения информационной безопасности ***Владеть (****или* ***Иметь опыт деятельности):*** эксплуатации ТКС на основных этапах жизненного цикла	***Знать:*** особенности различных этапов жизненного цикла ТКС ***Уметь:*** исходя их обширного перечня угроз реализовывать технологии обеспечения информационной безопасности ***Владеть (****или* ***Иметь опыт деятельности):*** эксплуатации ТКС на различных этапах жизненного цикла
	ПК-11.2 Выбирает перечень реализуемых	***Знать:*** перечень реализуемых телекоммуникационной системой технологий для	***Знать:*** структуру реализуемых телекоммуникационной системой технологий для	***Знать:*** структуру и особенности реализуемых телекоммуникационной системой

1	2	3	4	5
	телекоммуникационной системой технологий для удовлетворения требований по информационной безопасности	удовлетворения требований по информационной безопасности ***Уметь:*** соотносить отдельные технологии информационной безопасности существующим в ТКС уязвимостям ***Владеть (****или* ***Иметь опыт деятельности):*** реализации базовых технологий информационной безопасности	удовлетворения требований по информационной безопасности ***Уметь:*** соотносить основные технологии информационной безопасности существующим в ТКС уязвимостям ***Владеть (****или* ***Иметь опыт деятельности):*** реализации основных технологий информационной безопасности	технологий для удовлетворения требований по информационной безопасности ***Уметь:*** соотносить технологии информационной безопасности существующим в ТКС уязвимостям ***Владеть (****или* ***Иметь опыт деятельности):*** реализации стека технологий информационной безопасности
	ПК-11.3 Оценивает результат применения штатных средств обеспечения информационной безопасности	***Знать:*** шкалы результативности применения штатных средств обеспечения информационной безопасности ***Уметь:*** использовать количественные критерии результативности применения штатных средств обеспечения информационной безопасности ***Владеть (****или* ***Иметь опыт деятельности):*** навыками применения штатных средств обеспечения информационной безопасности	***Знать:*** критерии результативности применения штатных средств обеспечения информационной безопасности ***Уметь:*** формулировать количественные критерии результативности применения штатных средств обеспечения информационной безопасности ***Владеть (****или* ***Иметь опыт деятельности):*** навыками оценки результативности применения штатных средств обеспечения информационной безопасности	***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 деятельности):*** сформированными навыками оценки результативности применения различных средств обеспечения информационной безопасности
	ПК-11.4 Формулирует предложени	***Знать:*** базовые технологии, направленные на повышение	***Знать:*** основные технологии, направленные на повышение	***Знать:*** меры и технологии, направленные на повышение

1	2	3	4	5
	я по совершенствованию подсистем обеспечения информационной безопасности	защищённости процессов обработки информации в ТКС ***Уметь:*** определять отдельные меры и технологии, направленные на повышение защищённости процессов обработки информации в конкретной ТКС ***Владеть (****или* ***Иметь опыт деятельности):*** проведения отдельных процедур защиты информации в ТКС	защищённости процессов обработки информации в ТКС ***Уметь:*** определять меры и технологии, направленные на повышение защищённости процессов обработки информации в конкретной ТКС ***Владеть (****или* ***Иметь опыт деятельности):*** обеспечения процесса защиты информации в ТКС	защищённости процессов обработки информации в ТКС ***Уметь:*** определять меры и технологии, направленные на повышение защищённости процессов обработки информации в сложных ТКС ***Владеть (****или* ***Иметь опыт деятельности):*** обеспечения процесса защиты информации в сложных ТКС

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-1 завершающий	Дневник практики. Отчёт по практике с результатами измерений и отчётов
ПК-6 завершающий	Дневник практики. Отчет о практике. Доклад обучающегося на промежуточной аттестации (защита отчета о практике). Характеристика руководителя практики от организации управленческих качеств обучающегося.
ПК-7 завершающий	Дневник практики. Отчет о практике.

	Типовое задание № 1 по практической подготовке, предусматривающее выполнение обучающимся вида(ов) работ, связанного(ых) с будущей профессиональной деятельностью (задание конкретизируется с учетом особенностей конкретной профильной организации в Дневнике практики, в п.1.4 задания студенту): *Подготовьте паспорт объекта информатизации для проведения аттестационных испытаний по защите информации.* Ответы на вопросы по содержанию практики на промежуточной аттестации.
ПК-8 завершающий	Отчет о практике. Типовое задание № 2 по практической подготовке, предусматривающее выполнение обучающимся вида(ов) работ, связанного(ых) с будущей профессиональной деятельностью (задание конкретизируется с учетом особенностей конкретной профильной организации в Дневнике практики, в п.1.4 задания студенту): *разработать модель угроз для объекта информатизации, на котором происходит эксплуатация телекоммуникационной ситсемы.* Разработанные модели угроз Ответы на вопросы по содержанию практики на промежуточной аттестации.
ПК-9 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 (производственного контроля).* Графические материалы к отчету. Раздел отчета о практике – *Результаты проведенного мониторинга (и (или) производственного контроля) работоспособности ТКС.*
ПК-10 завершающий	Дневник практики. Разделы отчета о практике: – *Профили защиты используемых средств обеспечения информационной безопасности.* – *Защищённости ТКС.*
ПК-11 завершающий	Дневник практики. Отчета 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 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:

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

5) Абрамов, Г. В. Проектирование информационных систем : учебное пособие / Г. В. Абрамов, И. Медведкова, Л. Коробова. - Воронеж : Воронежский государственный университет инженерных технологий, 2012. - 172 с. - URL: http://biblioclub.ru/index.php?page=book&id=141626 (дата обращения 03.09.2021) . - Режим доступа: по подписке. - ISBN 978-5-89448-953-7. - Текст : электронный.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

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

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

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

9 Описание материально-технической базы, необходимой для проведения практики

Для проведения практики используется оборудование конкретной профильной организации, на базе которой она проводится: современная измерительная техника: устройства, позволяющие осуществлять контроль

защищённости, программные и аппаратные системы защиты информации, обрабатываемых в телекоммуникационных системах, и устройства, позволяющие фиксировать параметры микроклимата (м*ежсетевые экраны, роутеры, маршрутизаторы, коммутаторы, системы виброакустического зашумления, датчики , акустические излучатели, подавители «жучков» и беспроводных видеокамер , поисковые приборы, генераторы шума*);

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

м*ежсетевые экраны, роутеры, маршрутизаторы, коммутаторы, системы виброакустического зашумления, датчики , акустические излучатели, подавители «жучков» и беспроводных видеокамер , поисковые приборы, генераторы шума*

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

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

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

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

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

Определение места практики

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

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

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

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

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

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

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

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

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

Особенности содержания практики

Индивидуальные задания формируются руководителем практики от университета с учетом особенностей психофизического развития,

индивидуальных возможностей и состояния здоровья каждого конкретного обучающегося данной категории и должны соответствовать требованиям выполнимости и посильности.

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

Особенности организации трудовой деятельности обучающихся

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

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

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

Особенности руководства практикой

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

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

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

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

Особенности учебно-методического обеспечения практики

Учебные и учебно-методические материалы по практике представляются в различных формах так, чтобы инвалиды с нарушениями слуха получали информацию визуально (программа практики и индивидуальное задание на практику печатаются увеличенным шрифтом;

предоставляются видеоматериалы и наглядные материалы по содержанию практики), с нарушениями зрения – аудиально (например, с использованием программ-синтезаторов речи) или с помощью тифлоинформационных устройств.

Особенности проведения текущего контроля успеваемости и промежуточной аттестации

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

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

11 Лист дополнений и изменений, внесенных в программу практики

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