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 эксплуатационная 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 2021 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 2023 г., на заседании кафедры ИБ протокол №1 от 30.08.2023.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

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

1.1. Цель практики

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

1.2. Задачи практики

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

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

Вид практики – производственная.

Тип практики – эксплуатационная.

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

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

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

Обучающиеся, совмещающие обучение с трудовой деятельностью, вправе проходить практику по месту трудовой деятельности в случаях, если профессиональная деятельность, осуществляемая ими, соответствует

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*		
1	2	3	4
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;	ОПК-5.1; Разрабатывает проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации	***Знать:*** Правовые основы организации защиты конфиденциальной информации, задачи органов защиты информации; ***Уметь:*** применять действующую законодательную базу в области обеспечения информационной безопасности; классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации ***Владеть (****или* ***Иметь опыт деятельности):*** навыками работы с нормативными правовыми актами; навыками разработки проектов локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации.

1	2	3	4
		ОПК-5.2; Формулирует основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации	***Знать:*** Правовые нормы и стандарты по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации; принципы формирования политики информационной безопасности в автоматизированных системах ***Уметь:*** применять действующую законодательную базу по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации; разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации ***Владеть (****или* ***Иметь опыт деятельности):*** навыками работы с нормативными правовыми актами; навыками разработки проектов локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации.
		ОПК-5.3; Формулирует основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации	***Знать:*** Правовые нормы и стандарты по лицензированию в области обеспечения защиты информации и сертификации средств защиты; основные отечественные и зарубежные стандарты в области информационной безопасности; терминологию, основные руководящие и регламентирующие документы в области ЭВМ, комплексов и систем. ***Уметь:*** применять действующую законодательную базу в области обеспечения информационной

1	2	3	4
			безопасности при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации; разрабатывать проекты локальных правовых актов, инструкций, регламентов при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации. ***Владеть (****или* ***Иметь опыт деятельности):*** навыками работы с нормативными правовыми актами; навыками работы с технической документацией на ЭВМ и вычислительные системы; навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках.
		ОПК-5.4; Формулирует основные требования информационной безопасности при эксплуатации телекоммуникационной системы	***Знать:*** Правовые нормы и стандарты по защите конфиденциальной информации при эксплуатации телекоммуникационной системы. ***Уметь:*** применять действующую законодательную базу по защите конфиденциальной информации, при эксплуатации телекоммуникационной системы ***Владеть (****или* ***Иметь опыт деятельности):*** навыками работы с нормативными правовыми актами; навыками разработки проектов локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по защите конфиденциальной информации при эксплуатации телекоммуникационной системы
ОПК-6	Способен при решении профессиональных задач организовывать	ОПК-6.1 Разрабатывает модели угроз и модели нарушителя объекта	***Знать*** основные угрозы безопасности и модели нарушителя объекта информатизации ***Уметь:*** разрабатывать модели угроз и модели нарушителя объекта

1	2	3	4
	защиту информации ограниченного доступа в процессе функционирования сетей электросвязи в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	информатизации	информатизации ***Владеть (****или* ***Иметь опыт деятельности):*** навыками оценки угроз для объекта информатизации
		ОПК-6.2 Формулирует основные требования, предъявляемые к организации защиты информации ограниченного доступа	***Знать*** основные требования, предъявляемые к организации защиты информации ограниченного доступа угрозы безопасности и модели нарушителя объекта информатизации ***Уметь:*** разрабатывать требования, предъявляемые к организации защиты информации ограниченного доступа ***Владеть (****или* ***Иметь опыт деятельности):*** навыками формулирования основных требований, предъявляемых к организации защиты информации ограниченного доступа
		ОПК-6.3 Анализирует состав и функциональные возможности средств защиты информации телекоммуникационной системы в целях его совершенствования	***Знать*** состав и функциональные возможности средств защиты информации телекоммуникационной системы. ***Уметь:*** совершенствовать состав и функциональные возможности средств защиты информации телекоммуникационной системы ***Владеть (****или* ***Иметь опыт деятельности):*** навыками оценки функциональных возможностей средств защиты информации телекоммуникационной системы
		ОПК-6.4 Разрабатывает проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации	***Знать*** правовые нормы и стандарты для разработки инструкций, регламентов, положений и приказов, регламентирующих защиту информации ***Уметь:*** составлять проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации ***Владеть (****или* ***Иметь опыт деятельности):*** навыками организации документооборота в области защиты информации.
ОПК-9	Способен использовать программные, программно-	ОПК-9.1 Организует защиту информации от утечки по	***Знать:*** виды угроз и возможные каналы утечки конфиденциальной информации по техническим каналам.

1	2	3	4
	аппаратные и технические средства защиты информации при решении задач профессиональной деятельности	техническим каналам в телекоммуникационных системах	***Уметь:*** Выполнять требования нормативных и эксплуатационных документов (документации) по обеспечению защиты информации, передаваемой в телекоммуникационных системах и вскрытия каналов утечки информации, по организации мероприятий, направленных на защиту информации. ***Владеть:*** навыками применения технических средств защиты информации.
		ОПК-9.2 Проводит инструментальный контроль показателей технической защиты информации в телекоммуникационных системах и сетях	***Знать:*** классификацию, принципы, способы и порядок функционирования средств защиты информации, принципы организации проверок технических СЗИ, инструментальные средства проведения проверок технических СЗИ,. ***Уметь:*** применять средства контроля показателей технической защиты информации в соответствии с эксплуатационной документацией, анализировать. ***Владеть:*** навыками организации контрольных проверок технических СЗИ, эксплуатации средств контроля защиты информации в соответствии с эксплуатационной документацией.
		ОПК-9.3; Использует средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации	***Знать:*** комплекс мероприятий, технических мер и методов, направленных на повышение защищенности и снижения рисков нарушения безопасности телекоммуникационных систем и сетей. ***Уметь:*** применять средства защиты информации в соответствии с эксплуатационной документацией, применять известные методики оценки угроз, принимать технические меры, направленные на повышение защищенности и снижения рисков нарушения безопасности телекоммуникационных систем. ***Владеть:*** навыками эксплуатации средств защиты информации и анализа защищенности

1	2	3	4
			телекоммуникационных систем и сетей, методами проведения анализа угроз информационной безопасности.
		ОПК-9.4 Осуществляет автономную наладку технических и программных средств системы защиты информации автоматизированной системы	***Знать*** принципы построения современных технических и программных средств системы защиты информации***:*** ***Уметь:*** устанавливать и настраивать технические и программные средства защиты информации и их подсистем обеспечения информационной безопасности ***Владеть (****или* ***Иметь опыт деятельности):*** оценки эффективности функционирования технических и программных средств защиты информации и их подсистем
		ОПК-9.5 Применяет типовые программные средства резервирования и восстановления информации в автоматизированных системах	***Знать:*** знать номенклатуру регламентных работ по резервированию и восстановлению работоспособности устройств и программ ***Уметь:*** выполнять регламентные работы по восстановлению работоспособности устройств и программ ***Владеть (****или* ***Иметь опыт деятельности):*** эксплуатации программного и аппаратного обеспечения ТКС в различных режимах работы
ОПК-10	Способен использовать методы и средства криптографической защиты информации при решении задач профессиональной деятельности;	ОПК-10.1 Использует средства криптографической защиты информации в автоматизированных системах	***Знать***: механизмы решения типовых задач по криптографической защите информации; полный перечень данных, нужных при проектировании подсистем и средств обеспечения криптографической безопасности информации; принципы работы программных, программно-аппаратных криптографических средств зашиты информации; ***Уметь***: проводить комплексный анализ всех исходных данных для построения криптографических систем защиты информации; оценивать область применения конкретных механизмов криптографической защиты для

1	2	3	4
			построения защищенных информационных систем. ***Владеть***: навыками применения криптографических программных средств системного, прикладного и специального назначения для решения задач по построению систем криптографической защиты безопасности;
ОПК-16	Способен проектировать защищенные телекоммуникационные системы и их элементы, проводить анализ проектных решений по обеспечению заданного уровня безопасности и требуемого качества обслуживания телекоммуникационных систем, разрабатывать необходимую техническую документацию с учетом действующих нормативных и методических документов, проводить подготовку исходных данных для технико-экономического обоснования соответствующих проектных решений	ОПК-16.1 Формирует исходные данные для выполнения технико-экономического обоснования проектируемой телекоммуникационной системы	***Знать:*** - основы формирования исходных данных для телекоммуникационных задач; - основы экономического обоснования проекта. ***Уметь:*** - анализировать исходные данные для обоснования целесообразности разработки проекта; - анализировать предметную область и создавать декларативное описание задачи; - применять принципы выявления ключевых параметров работы информационной системы; ***Владеть (****или* ***Иметь опыт деятельности):*** - приемами анализа полноты и корректности ключевых параметров эксплуатации;
		ОПК-16.2 Формирует требования к проектируемой системе с учетом анализа угроз защищаемым активам телекоммуникационной системы	***Знать:*** - технологии повышения защищенности распределенных информационных систем; ***Уметь:*** - выполнять определять характер угрозы и масштабы последствий; - проектировать регламент защищенного взаимодействия компонентов ТЛК системы; - минимизировать последствия ущерба за счет интеграции средств защиты. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками разработки компонентов ТЛК систем; - навыками обеспечения совместимого взаимодействия

1	2	3	4
			отдельных модулей;
		ОПК-16.3 Проводит анализ показателей качества проектируемых сетей и систем телекоммуникаций	***Знать:*** - особенности вывода промежуточных значений в ходе работы модулей; - основы использования управляющих директив. ***Уметь:*** - выполнять отладку приложения в пошаговом режиме и с контрольными точками; - минимизировать количество потенциальных нештатных ситуаций работы программы. ***Владеть (****или* ***Иметь опыт деятельности):*** - установки директив, определяющих работу программных модулей; - технологией ведения протокола работы системы с выводом промежуточных результатов обработки данных.
		ОПК-16.4 Оценивает защищенность сетевого оборудования и телекоммуникационных систем	***Знать:*** - основы работы в режиме пошаговой отладки передачи конфиденциальных данных в информационной системе; - основы шифрования потоков данных; - основы использования средств защиты информации. ***Уметь:*** - организовать безопасную работу в масштабе вычислительной сети; - выводить сообщения в случае возникновения нештатных ситуаций работы информационной системы; - интегрировать средства защиты на программном уровне. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками установки программных средств защиты; - навыками оценки защищенности информационной системы с учетом возможных угроз.
		ОПК-16.5 Создаёт	***Знать:***

1	2	3	4
		компоненты защищенных телекоммуникационных систем	- этапы разработки программного обеспечения; - модели жизненного цикла программного обеспечения; ***Уметь:*** **-** разрабатывать базовые компоненты ТЛК систем; - принимать обоснованные решения по выбору технологий разработки; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками разработки компонентов ТЛК систем на программном уровне; - навыками интеграции отдельных компонентов в состав единой распределенной системы.
ОПК-9.1	Способен формировать, внедрять и обеспечивать функционирование системы менеджмента информационной безопасности телекоммуникационных систем и сетей	ОПК-9.1.1 Составляет отчеты по результатам проверок защищенности телекоммуникационных систем и сетей	***Знать:*** содержание журналов аудита информационной безопасности телекоммуникационных систем и сетей ***Уметь:*** использовать технические средства ведения журналов аудита информационной безопасности телекоммуникационных систем и сетей ***Владеть (****или* ***Иметь опыт деятельности):*** навыками анализа журналов аудита информационной безопасности телекоммуникационных систем и сетей
		ОПК-9.1.2 Выработки и реализации управленческих решений по обеспечению защиты телекоммуникационных систем и сетей	***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 последовательности ***Владеть (****или* ***Иметь опыт деятельности):*** использования отдельных технологий обеспечения информационной безопасности в ТКС
		ОПК-9.1.3 Разрабатывает рекомендации по эксплуатации системы защиты	***Знать:*** порядок эксплуатации средств обеспечения информационной безопасности телекоммуникационных систем сетей

1	2	3	4
		информации	***Уметь:*** объединять отдельные технологии и процедуры по обеспечению информационной безопасности в последовательности ***Владеть (****или* ***Иметь опыт деятельности):*** навыками эксплуатации средств обеспечения информационной безопасности телекоммуникационных систем сетей
		ОПК-9.1.4 Оценивает рисков, связанных с осуществлением угроз безопасности	***Знать:*** каналы утечки конфиденциальной информации по техническим каналам, основные тактико-технические характеристики, принципы построения технических средств передачи и защиты информации, виды сигналов и способы распространения, принципы и способы организации системы защиты информации на объектах информатизации. ***Уметь:*** Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями инструкций, эксплуатационной документации. ***Владеть:*** навыками оценки рисков, связанных с осуществлением угроз безопасности.
ОПК-9.2	Способен реализовывать комплекс организационных мероприятий по обеспечению информационной безопасности и устойчивости телекоммуникационных систем и сетей	ОПК-9.2.1 Проводит предусмотренные регламентом работы по восстановлению процесса и параметров функционирования телекоммуникационных систем и сетей	***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 аппаратного обеспечения ТКС в различных режимах работы
		ОПК-9.2.2 Проводить текущий контроль показателей и процесса функционирования телекоммуникационных систем и сетей	***Знать:*** основные признаки возникновения ошибок в телекоммуникационных системах и сетях ***Уметь:*** в процессе эксплуатации фиксировать режимы работы в телекоммуникационных системах и сетях, отличные от штатных

1	2	3	4
			Владеть (или Иметь опыт деятельности): навыками обнаружения сбоев и отказов в в телекоммуникационных системах и сетях
		ОПК-9.2.3 Использует средства измерений и контроля процесса и параметров функционирования телекоммуникационных систем и сетей	***Знать:*** Профили защиты инструментальные средства обеспечения защиты информации телекоммуникационных систем. ***Уметь:*** Осуществлять рациональный выбор средств реализации профилей защиты. ***Владеть:*** Навыками контроля процесса и параметров функционирования телекоммуникационных систем и сетей.
ОПК-9.3	Способен проводить мониторинг защищенности сетевых ресурсов и формировать отчеты по выявленным уязвимостям	ОПК-9.3.1 Использует сканеры безопасности телекоммуникационных систем и сетей	***Знать:*** классификацию, виды и типы инструментальных средств контроля защищенности информации в телекоммуникационных системах; Методы и способы контроля защищенности информации; ***Уметь:*** применять инструментальные средства контроля защищенности информации в телекоммуникационных системах; производить оценку полученных результатов; сопоставлять результаты измерений с требуемыми значениями. ***Владеть:*** навыками инструментального контроля защищенности информации в автоматизированных системах; анализа защищенности телекоммуникационных систем; навыками выбора инструментальных средств контроля защищенности информации; навыками интерпретации результатов измерений и определения подхода для повышения защищенности телекоммуникационных систем.
		ОПК-9.3.2 Применяет методы анализа	***Знать:*** номенклатуру, принципы организации, технические характеристики средств

1	2	3	4
		защищенности телекоммуникационных систем и сетей	защищенности телекоммуникационных систем и сетей ***Уметь:*** использовать функциональные возможности компонентов телекоммуникационных систем и сетей для анализа защищенности телекоммуникационных систем и сетей ***Владеть (или Иметь опыт деятельности):*** навыками эксплуатации телекоммуникационных систем сетей в различных состояних защищённости
		ОПК-9.3.3 Проводит настройку средств автоматического реагирования на попытки несанкционированного доступа	***Знать:*** классификацию, виды и типы угроз безопасности телекоммуникационных систем, принципы построения средств защиты информации; основные компоненты телекоммуникационных систем объекта информатизации; компоненты, назначение и функциональные особенности средств автоматического реагирования на попытки несанкционированного доступа. ***Уметь:*** определять параметры конфигурирования программно-аппаратных средств реагирования на попытки несанкционированного доступа. ***Владеть:*** навыками защиты информации в компьютерных сетях; навыками конфигурирования программно-аппаратных средств реагирования на попытки несанкционированного доступа.

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 обязательную часть блока 2 «Практика» основной профессиональной образовательной программы – программы специалитета 10.05.02 Информационная

безопасность телекоммуникационных систем, специализация «Управление безопасностью телекоммуникационных систем и сетей». Практика проходит на 6 курсе в 11 семестре.

Объем производственной преддипломной практики, установленный учебным планом, – 6 зачетных единиц, продолжительность – 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 36 часов (часы указаны в учебном плане в графе «Пр»), работа обучающегося в иных формах – 288 часов (часы указаны в учебном плане в графе «СР»).

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

Таблица 4 – Этапы и содержание практики

№ п/п	Этапы практики	Содержание практики	Трудоемкость (час)
1	Подготовительный этап	Решение организационных вопросов: 1) распределение обучающихся по местам практики; 2) знакомство с целью, задачами, программой, порядком прохождения практики; 3) получение заданий от руководителя практики от университета; 4) информация о требованиях к отчетным документам по практике; 5) первичный инструктаж по 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.	
		Изучение нормативных правовых актов профильной организации по обеспечению информационной безопасности (политика безопасности профильной организации, положения, приказы, инструкции, должностные обязанности, памятки и др.).	3
2.2	Практическая подготовка обучающихся *(непосредственное выполнение обучающимися видов работ, связанных с будущей профессиональной деятельностью)*	Самостоятельное проведение мониторинга и (или) производственного контроля эксплуатации средств защиты информации в ТКС. Организация работы 2-3 человек и руководство их работой в процессе проведения мониторинга безопасности ТКС. Создание плана работы коллектива из 3 – 4 человек, реализующего политику безопасности в ТКС	90.
		Самостоятельная обработка и систематизация полученных данных с помощью профессиональных программных комплексов и информационных технологий. *Формирование систематизированной инструкции по эксплуатации конкретного средства защиты информации в конкретной ТКС.* Представление результатов мониторинга руководителю практики от организации	
		Самостоятельное проведение уценки угроз информационной безопасности, возможных каналов утечек конфиденциальных данных в ТКС. Оценка рисков информационной безопасности. Представление результатов анализа и обоснование оценки руководителю практики от организации.	

		Самостоятельная подготовка рекомендаций по повышению уровня информационной безопасности предприятия. *Организация работы 2-3 человек и руководство их работой в процессе подготовки рекомендаций по проведению регламентных работ по обнаружению уязвимостей ТКС.* Представление своих рекомендаций руководителю практики от организации.	
		Самостоятельное составление рекомендаций по отказоустойчивой эксплуатации защищённых ТКС. Представление перечня средств и мер по обеспечению отказоустойчивости системы.	
3	Заключительный этап	Оформление дневника практики.	36
		Составление отчета о практике.	
		Подготовка графических материалов для отчета.	
		Представление дневника практики и защита отчета о практике на промежуточной аттестации.	

5 Указание форм отчетности по практике

Формы отчетности студентов о прохождении производственной производственной практики:

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

– отчет о практике.

Структура отчета о производственной преддипломной практике:

1) Титульный лист.

2) Содержание.

3) Введение. Цель и задачи практики. Общие сведения о предприятии, на котором проходила практика.

4) Основная часть отчета.

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

– Основные нормативные правовые акты предприятия по обеспечению информационной безопасности.

– Анализ результатов оценки эффективности применения средств обеспечения информационной безопасности.

– Оценка соответствия рисков информационной безопасности ТКС применяемым технологиям.

– Рекомендации по повышению уровня информационной безопасности предприятия.

– Краткосрочный и долгосрочный прогноз развития ситуации.

5) Заключение. Выводы о достижении цели и выполнении задач практики.

6) Список использованной литературы и источников.

7) Приложения (иллюстрации, таблицы, карты и т.п.).

Отчет должен быть оформлен в соответствии с:

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

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

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

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

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

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

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

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

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

6 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по практике

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

Таблица 6.1 – Этапы формирования компетенций

Код и наименование компетенции	Этапы* формирования компетенций и дисциплины (модули), практики, НИР, при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
ОПК-5	Организационное и правовое обеспечение информационной безопасности		Производственная эксплуатационная практика
ОПК-6	Организационное и правовое	Управление информационной безопасностью	Производственная эксплуатационная

	обеспечение информационной безопасности	телекоммуникационных систем	практика
ОПК-9	Защита информации от утечки по техническим каналам	Программно-аппаратные средства защиты информации	Производственная эксплуатационная практика
ОПК-10	Учебная практика (учебно-лабораторный практикум) Методы и средства криптографической защиты информации	Программно-аппаратные средства защиты информации Защита информации от утечки по техническим каналам	Производственная эксплуатационная практика
ОПК-16	Проектирование защищённых телекоммуникационных систем		Производственная эксплуатационная практика
ОПК-9.1	Управление информационной безопасностью телекоммуникационных систем		Производственная эксплуатационная практика
ОПК-9.2	Защита информации в телекоммуникационных сетях		Производственная эксплуатационная практика
ОПК-9.3	Мониторинг безопасности телекоммуникационных сетей		Производственная эксплуатационная 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
ОПК–5/ завершающий	ОПК-5.1; Разрабатывает проекты локальных правовых актов, инструкций, регламентов и организаци	Знать: -стандарты в области информационной безопасности; Уметь: - сопоставлять характеристики правового	Знать: - методологические подходы применения нормативных документов при оценке защищённости	Знать: - принципы формирования комплексных отчётов по аудиту информационной безопасности; Уметь:

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

1	2	3	4	5
	ет основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации	- основные нормативные правовые документы. Уметь: - ориентироваться в системе законодательства и нормативных правовых актов в области защиты информации. Владеть: - навыками поиска необходимых нормативных и законодательных документов и навыками работы с ними в профессиональной деятельности	- нормативно правовые документы. Уметь: - использовать нормативно правовые акты в задачах защиты информации Владеть: - навыками поиска необходимых нормативных и законодательных документов и навыками анализа результатов их применения.	- Российские и международные нормативно правовые документы в области защиты информации. Уметь: - разрабатывать рекомендации по применению нормативно правовых документов в области защиты информации. Владеть: - навыками разработки организационно-распорядительной документации на объекте информатизации
	ОПК-5.4; Формулирует основные требования информационной безопасности при эксплуатации телекоммуникационной системы	Знать*:* Правовые нормы и стандарты по защите конфиденциальной информации при эксплуатации телекоммуникационной системы. Уметь: применять действующую законодательную базу по защите конфиденциальн	Знать*:* Правовые нормы и стандарты по защите конфиденциальной информации при эксплуатации телекоммуникационной системы. Уметь: применять действующую законодательную базу по защите конфиденциальн	Знать*:* Правовые нормы и стандарты по защите конфиденциальной информации при эксплуатации телекоммуникационной системы. Уметь: применять действующую законодательную базу по защите конфиденциальн

1	2	3	4	5
		ой информации, при эксплуатации телекоммуникационной системы Владеть (или Иметь опыт деятельности): навыками работы с нормативными правовыми актами;	ой информации, при эксплуатации телекоммуникационной системы Владеть (или Иметь опыт деятельности): навыками работы с нормативными правовыми актами; навыками разработки проектов локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по защите конфиденциальной информации при эксплуатации телекоммуникационной системы	ой информации, при эксплуатации телекоммуникационной системы Владеть (или Иметь опыт деятельности): навыками работы с нормативными правовыми актами; навыками разработки проектов локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по защите конфиденциальной информации при эксплуатации телекоммуникационной системы; навыками анализа качества разработанных документов.
ОПК-6 завершающий	Разрабатывает модели угроз и модели нарушителя объекта информатизации	***Знать*** основные угрозы безопасности нарушителя объекта информатизации ***Уметь:*** разрабатывать модели угроз и	***Знать*** основные угрозы безопасности объекта информатизации ***Уметь:*** разрабатывать модели угроз и модели нарушителя	***Знать*** основные угрозы безопасности и модели нарушителя объекта информатизации ***Уметь:*** разрабатывать модели угроз и

1	2	3	4	5
		модели нарушителя объекта информатизации ***Владеть (****или* ***Иметь опыт деятельности):*** навыками использования моделей угроз и нарушителя	объекта информатизации ***Владеть (****или* ***Иметь опыт деятельности):*** навыками оценки угроз для объекта информатизации	модели нарушителя объекта информатизации ***Владеть (****или* ***Иметь опыт деятельности):*** навыками оценки угроз для объекта информатизации
	Формулирует основные требования, предъявляемые к организации защиты информации ограниченного доступа	***Знать*** основные требования, предъявляемые к организации защиты информации ограниченного доступа ***Уметь:*** формулировать требования, предъявляемые к организации защиты информации ограниченного доступа ***Владеть (****или* ***Иметь опыт деятельности):*** навыками формулирования основных требований, предъявляемых к организации защиты информации ограниченного доступа	***Знать*** требования, предъявляемые к организации защиты информации ограниченного доступа объекта информатизации ***Уметь:*** разрабатывать требования, предъявляемые к организации защиты информации ограниченного доступа ***Владеть (****или* ***Иметь опыт деятельности):*** навыками формулирования основных требований, предъявляемых к организации защиты информации ограниченного доступа	***Знать*** требования, предъявляемые к организации защиты информации ограниченного доступа угрозы безопасности и модели нарушителя объекта информатизации ***Уметь:*** разрабатывать требования, предъявляемые к организации защиты информации ограниченного доступа ***Владеть (****или* ***Иметь опыт деятельности):*** навыками формулирования требований, предъявляемых к организации защиты информации ограниченного доступа
	Анализирует состав и функциональные возможности средств защиты информации телекоммун	***Знать*** основной состав и функциональные возможности средств защиты информации телекоммуникационной системы. ***Уметь:*** совершенствовать	***Знать*** состав и функциональные возможности средств защиты информации телекоммуникационной системы. ***Уметь:*** совершенствовать состав и	***Знать*** состав и функциональные возможности средств защиты информации телекоммуникационной системы. ***Уметь:*** совершенствовать состав и

1	2	3	4	5
	икационной системы в целях его совершенствования	состав и функциональные возможности средств защиты информации телекоммуникационной системы ***Владеть (****или* ***Иметь опыт деятельности):*** навыками оценки функциональных возможностей средств защиты информации телекоммуникационной системы	функциональные возможности средств защиты информации телекоммуникационной системы ***Владеть (****или* ***Иметь опыт деятельности):*** навыками оценки функциональных возможностей средств защиты информации телекоммуникационной системы	функциональные возможности средств защиты информации телекоммуникационной системы ***Владеть (****или* ***Иметь опыт деятельности):*** навыками оценки функциональных возможностей средств защиты информации телекоммуникационной системы
	Разрабатывает проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации и ограниченного доступа в организации	***Знать*** основные правовые нормы и стандарты для разработки инструкций, регламентов, положений и приказов, регламентирующих защиту информации ***Уметь:*** составлять проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации ***Владеть (****или* ***Иметь опыт деятельности):*** навыками организации документооборота в области защиты информации.	***Знать*** правовые нормы и стандарты для разработки инструкций, регламентов, положений и приказов, регламентирующих защиту информации ***Уметь:*** составлять проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации ***Владеть (****или* ***Иметь опыт деятельности):*** навыками организации документооборота в области защиты информации.	***Знать*** правовые нормы и стандарты для разработки инструкций, регламентов, положений и приказов, регламентирующих защиту информации ***Уметь:*** составлять проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации ***Владеть (****или* ***Иметь опыт деятельности):*** навыками организации документооборота в области защиты информации; навыками оценки качества разработанных документов.

1	2	3	4	5
ОПК-9/ завершающий	ОПК-9.1 Организует защиту информации от утечки по техническим каналам в телекоммуникационных системах	Знать: виды угроз и возможные каналы утечки конфиденциальной информации по техническим каналам. Уметь: выполнять требования нормативных и эксплуатационных документов (документации) по обеспечению защиты информации в телекоммуникационных системах и вскрытия каналов утечки информации, по организации мероприятий, направленных на защиту информации. Владеть: навыками разработки нормативных и технических документов по организации защиты информации в телекоммуникационных системах.	Знать: основные тактико-технические характеристики, принципы построения технических средств передачи и защиты информации, виды сигналов и способы распространения радиоволн, принципы и способы организации системы защиты информации. Уметь: разрабатывать нормативную документацию по выполнению требований защиты в телекоммуникационных системах. Владеть: навыками применения технических средств защиты информации.	Знать: порядок и алгоритм проведения организационных мероприятий на объектах информатизации. Функциональные обязанности по организации мероприятий по защите информации в телекоммуникационных системах. Уметь: осуществлять выбор технических средств защиты информации в зависимости от условий эксплуатации в телекоммуникационных систем. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями инструкций, эксплуатационной документации. Владеть: навыками проведения организационных мероприятий по вскрытию уязвимых мест систем обеспечения защиты информации телекоммуникационных систем.

1	2	3	4	5
	ОПК-9.2 Проводит инструментальный контроль показателей технической защиты информации в телекоммуникационных системах и сетях	Знать: классификацию, принципы, способы и порядок функционирования средств защиты информации, принципы организации проверок технических СЗИ, инструментальные средства проведения проверок технических СЗИ. Уметь: анализировать нормативную документацию, регламентирующую порядок проведения контроля защиты информации. угрозы. Владеть: навыками организации контрольных проверок технических СЗИ, эксплуатации средств защиты информации и средств контроля защиты информации в соответствии с эксплуатационной документацией.	Знать: основные угрозы, предотвращаемые, СЗИ; виды, методы и средства контроля защиты информации. Уметь: организовать комплекс мероприятий контроля защиты информации, в соответствии регламентирующими документами. Владеть: требованиями нормативной документации, регламентирующей порядок проведения контроля защиты информации.	Знать: нормативные документы регламентирующие порядок проведения контроля защиты информации, комплекс мероприятий, проводимых в ходе контроля защиты информации.Уметь: применятьсредства защиты информации и средства контроля защиты информации в соответствии с эксплуатационной документацией. Владеть: навыками применения комплекса мероприятий контроля показателей технической защиты информации в телекоммуникационных системах и сетях.
	ОПК-9.3; Использует средства защиты информации от утечки по техническим каналам и контроля	Знать: классификацию, принципы, способы и порядок функционирования средств защиты информации, принципы организации проверок	Знать: основные угрозы, предотвращаемые, СЗИ; виды, методы и средства контроля защиты информации. Уметь: организовать комплекс	Знать: нормативные документы регламентирующие порядок проведения контроля защиты информации, комплекс мероприятий,

1	2	3	4	5
	эффективности защиты информации	технических СЗИ, инструментальные средства проведения проверок технических СЗИ. Уметь: анализировать нормативную документацию, регламентирующую порядок проведения контроля защиты информации. Владеть: навыками организации контрольных проверок технических СЗИ, эксплуатации средств защиты информации и средств контроля защиты информации в соответствии с эксплуатационной документацией.	мероприятий контроля эффективности защиты информации, в соответствии регламентирующими документами. Владеть: требованиями нормативной документации, регламентирующей порядок проведения контроля защиты информации.	проводимых в ходе контроля эффективности защиты информации. Уметь: применятьсредства защиты информации и средства контроля защиты информации в соответствии с эксплуатационной документацией. Владеть: навыками применения комплекса мероприятий контроля эффективности защиты информации.
	ОПК-9.4 Осуществляет автономную наладку технических и программных средств системы защиты информации и автоматизированной системы	***Знать*** номенклатуру современных технических и программных средств системы защиты информации***:*** ***Уметь:*** устанавливать и настраивать некоторые технические и программные средства защиты информации и их подсистем обеспечения информационной	***Знать*** принципы построения современных технических и программных средств системы защиты информации***:*** ***Уметь:*** устанавливать и настраивать наиболее распространённые технические и программные средства защиты информации и их подсистем обеспечения	***Знать*** принципы построения, особенности функционирования и критерии оценки эффективности применения современных технических и программных средств системы защиты информации***:*** ***Уметь:*** устанавливать и настраивать технические и программные средства защиты

1	2	3	4	5
		безопасности ***Владеть (или Иметь опыт деятельности):*** эксплуатации технических и программных средств защиты информации и их подсистем	информационной безопасности ***Владеть (или Иметь опыт деятельности):*** оценки качественных и количественных критериев качества функционирования технических и программных средств защиты информации и их подсистем	информации и их подсистем обеспечения информационной безопасности ***Владеть (или Иметь опыт деятельности):*** оценки эффективности функционирования технических и программных средств защиты информации и их подсистем
	ОПК-9.5 Применяет типовые программные средства резервирования и восстановления информации в автоматизированных системах	***Знать:*** знать номенклатуру регламентных работ по резервированию и восстановлению работоспособности устройств и программ ***Уметь:*** выполнять этапы регламентных работ по восстановлению работоспособности устройств и программ ***Владеть (или Иметь опыт деятельности):*** эксплуатации программного и аппаратного обеспечения ТКС в базовых режимах работы	***Знать:*** знать принципы организации регламентных работ по резервированию и восстановлению работоспособности устройств и программ ***Уметь:*** выполнять регламентные работы по восстановлению работоспособности устройств и программ ***Владеть (или Иметь опыт деятельности):*** эксплуатации программного и аппаратного обеспечения ТКС в различных режимах работы	***Знать:*** знать принципы организации и особенности проведения регламентных работ по резервированию и восстановлению работоспособности устройств и программ ***Уметь:*** **грамотно и эффективно** выполнять регламентные работы по восстановлению работоспособности устройств и программ ***Владеть (или Иметь опыт деятельности):*** эксплуатации программного и аппаратного обеспечения ТКС в нетиповых режимах работы
ОПК-10/ завершающий	ОПК-10.1 Использует средства криптографической	Знать: -простейшие методы работы с программным обеспечением.	Знать: -принципы работы программных, программно – аппаратных средств	Знать: -принципы работы программных, программно – аппаратных средств

1	2	3	4	5
	защиты информации в автоматизированных системах	Уметь: -выполнять работы по установке и настройке программного обеспечения Владеть: -навыками сбора необходимой информации по работе с программных, программно – аппаратных средств криптографической защиты информации.	и технических средств зашиты информации Уметь: -проводить анализ полученных исходных данных Владеть: -навыками подбора наилучший метода решения задачи криптографической защиты информации.	и технических средств криптографической зашиты информации Уметь: -применять все полученные знания при решении разного рода задач по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации Владеть: -достаточным количеством информации для решения возникающих проблем криптографической защиты информации
ОПК-16/ завершающий	ОПК-16.1 Формирует исходные данные для выполнения технико-экономического обоснования проектируемой телекоммуникационной системы	***Знать:*** - основы экономического обоснования проекта. ***Уметь:*** - анализировать исходные данные для обоснования целесообразности разработки проекта; - применять принципы выявления ключевых параметров работы информационной системы; ***Владеть (****или* ***Иметь опыт деятельности):*** - приемами анализа полноты и корректности ключевых параметров эксплуатации;	***Знать:*** - основы формирования исходных данных для телекоммуникационных задач; ***Уметь:*** - анализировать исходные данные для обоснования целесообразности разработки проекта; - применять принципы выявления ключевых параметров работы информационной системы; ***Владеть (****или* ***Иметь опыт деятельности):*** - приемами анализа полноты и корректности ключевых параметров	***Знать:*** - основы формирования исходных данных для телекоммуникационных задач; - основы экономического обоснования проекта. ***Уметь:*** - анализировать исходные данные для обоснования целесообразности разработки проекта; - анализировать предметную область и создавать декларативное описание задачи; - применять принципы выявления ключевых параметров работы информационной системы;

1	2	3	4	5
			эксплуатации;	***Владеть (****или* ***Иметь опыт деятельности):*** - приемами анализа полноты и корректности ключевых параметров эксплуатации;
	ОПК-16.2 Формирует требования к проектируемой системе с учетом анализа угроз защищаемым активам телекоммуникационной системы	***Знать:*** - технологии повышения защищенности распределенных информационных систем; ***Уметь:*** - проектировать регламент защищенного взаимодействия компонентов ТЛК системы; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками обеспечения совместимого взаимодействия отдельных модулей;	***Знать:*** - технологии повышения защищенности распределенных информационных систем; ***Уметь:*** - выполнять определять характер угрозы и масштабы последствий; - минимизировать последствия ущерба за счет интеграции средств защиты. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками разработки компонентов ТЛК систем; - навыками обеспечения совместимого взаимодействия отдельных модулей;	***Знать:*** - технологии повышения защищенности распределенных информационных систем; ***Уметь:*** - выполнять определять характер угрозы и масштабы последствий; - проектировать регламент защищенного взаимодействия компонентов ТЛК системы; - минимизировать последствия ущерба за счет интеграции средств защиты. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками разработки компонентов ТЛК систем; - навыками обеспечения совместимого взаимодействия отдельных модулей;
	ОПК-16.3 Проводит анализ показателей качества проектируемых сетей и систем телекоммуникаций	***Знать:*** - основы использования управляющих директив. ***Уметь:*** - минимизировать количество потенциальных нештатных ситуаций работы программы.	***Знать:*** - особенности вывода промежуточных значений в ходе работы модулей; ***Уметь:*** - минимизировать количество потенциальных нештатных ситуаций работы программы.	***Знать:*** - особенности вывода промежуточных значений в ходе работы модулей; - основы использования управляющих директив. ***Уметь:*** - выполнять отладку

1	2	3	4	5
		Владеть (или Иметь опыт деятельности): - технологией ведения протокола работы системы с выводом промежуточных результатов обработки данных.	***Владеть (или Иметь опыт деятельности):*** - установки директив, определяющих работу программных модулей;	приложения в пошаговом режиме и с контрольными точками; - минимизировать количество потенциальных нештатных ситуаций работы программы. ***Владеть (или Иметь опыт деятельности):*** - установки директив, определяющих работу программных модулей; - технологией ведения протокола работы системы с выводом промежуточных результатов обработки данных.
	ОПК-16.4 Оценивает защищенность сетевого оборудования и телекоммуникационных систем	***Знать:*** - основы работы в режиме пошаговой отладки передачи конфиденциальных данных в информационной системе; - основы шифрования потоков данных; ***Уметь:*** - выводить сообщения в случае возникновения нештатных ситуаций работы информационной системы; - интегрировать средства защиты на программном уровне. ***Владеть (или Иметь опыт деятельности):*** - навыками оценки защищенности информационной системы с учетом возможных угроз.	***Знать:*** - основы шифрования потоков данных; - основы использования средств защиты информации. ***Уметь:*** - организовать безопасную работу в масштабе вычислительной сети; - выводить сообщения в случае возникновения нештатных ситуаций работы информационной системы; - интегрировать средства защиты на программном уровне. ***Владеть (или Иметь опыт деятельности):*** - навыками установки программных	***Знать:*** - основы работы в режиме пошаговой отладки передачи конфиденциальных данных в информационной системе; - основы шифрования потоков данных; - основы использования средств защиты информации. ***Уметь:*** - организовать безопасную работу в масштабе вычислительной сети; - выводить сообщения в случае возникновения нештатных ситуаций работы информационной системы; - интегрировать средства защиты на

1	2	3	4	5
			средств защиты;	программном уровне. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками установки программных средств защиты; - навыками оценки защищенности информационной системы с учетом возможных угроз.
	ОПК-16.5 Создаёт компоненты защищенных телекоммуникационных систем	***Знать:*** - модели жизненного цикла программного обеспечения; ***Уметь:*** **-** разрабатывать базовые компоненты ТЛК систем; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками интеграции отдельных компонентов в состав единой распределенной системы.	***Знать:*** - этапы разработки программного обеспечения; - модели жизненного цикла программного обеспечения; ***Уметь:*** - принимать обоснованные решения по выбору технологий разработки; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками разработки компонентов ТЛК систем на программном уровне; - навыками интеграции отдельных компонентов в состав единой распределенной системы.	***Знать:*** - этапы разработки программного обеспечения; - модели жизненного цикла программного обеспечения; ***Уметь:*** **-** разрабатывать базовые компоненты ТЛК систем; - принимать обоснованные решения по выбору технологий разработки; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками разработки компонентов ТЛК систем на программном уровне; - навыками интеграции отдельных компонентов в состав единой распределенной системы.
ОПК-9.1/ завершающий	ОПК-9.1.1 Составляет отчеты по результатам проверок защищенности телекоммуникационных	***Знать:*** содержание журналов аудита информационной безопасности телекоммуникационных систем и сетей ***Уметь:***	***Знать:*** Структуру и порядок ведения журналов аудита информационной безопасности телекоммуникационных систем и сетей	***Знать:*** Принципы ведения, обработки и структуру журналов аудита информационной безопасности телекоммуникационных систем и

1	2	3	4	5
	систем и сетей	использовать технические средства ведения журналов аудита информационной безопасности телекоммуникационных систем и сетей ***Владеть (или Иметь опыт деятельности):*** навыками ведения журналов аудита информационной безопасности телекоммуникационных систем и сетей	***Уметь:*** использовать средства обработки журналов аудита информационной безопасности телекоммуникационных систем и сетей ***Владеть (или Иметь опыт деятельности):*** навыками восстановления хронологии событий в результате обработки журналов аудита информационной безопасности телекоммуникационных систем и сетей	сетей ***Уметь:*** определять порядок анализа журналов аудита информационной безопасности телекоммуникационных систем и сетей ***Владеть (или Иметь опыт деятельности):*** навыками анализа журналов аудита информационной безопасности телекоммуникационных систем и сетей
	ОПК-9.1.2 Выработки и реализации управленческих решений по обеспечению защиты телекоммуникационных систем и сетей	***Знать:*** отдельные угроз, на нейтрализацию которых направлена та или иная мера 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	***Знать:*** перечень угроз, на нейтрализацию которых направлена та или иная мера по защите информации ***Уметь:*** проводить комплексы мероприятий по обеспечению информационной безопасности в логически структурированные последовательности ***Владеть (или Иметь опыт деятельности):*** использования технологий обеспечения информационной безопасности в ТКС	***Знать:*** методику сопоставления угроз и мер 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		
	ОПК-9.1.3 Разрабатывает рекомендации по эксплуатации системы защиты информации	***Знать:*** порядок эксплуатации средств обеспечения информационной безопасности телекоммуникационных систем сетей ***Уметь:*** проводить отдельные процедуры по обеспечению информационной безопасности в последовательности ***Владеть (или Иметь опыт деятельности):*** навыками эксплуатации некоторых средств обеспечения информационной безопасности телекоммуникационных систем сетей	***Знать:*** порядок и правила эксплуатации средств обеспечения информационной безопасности телекоммуникационных систем сетей ***Уметь:*** проводить последовательности процедур по обеспечению информационной безопасности в последовательности ***Владеть (или Иметь опыт деятельности):*** навыками эксплуатации средств обеспечения информационной безопасности телекоммуникационных систем сетей	***Знать:*** порядок, правила и особенности эксплуатации средств обеспечения информационной безопасности телекоммуникационных систем сетей ***Уметь:*** объединять отдельные технологии и процедуры по обеспечению информационной безопасности в последовательности ***Владеть (или Иметь опыт деятельности):*** навыками эксплуатации разнообразных средств обеспечения информационной безопасности телекоммуникационных систем сетей
ОПК-9.2/ завершающий	ОПК-9.2.1 Проводит предусмотренные регламентом работы по восстановлению процесса и параметров функционирования телекоммуникационных систем и сетей	***Знать:*** основные каналы утечки конфиденциальной информации по техническим каналам, основные тактико-технические характеристики, принципы построения технических средств передачи и защиты информации,. ***Уметь:*** Осуществлять эксплуатацию технических	***Знать:*** каналы утечки конфиденциальной информации по техническим каналам, основные тактико-технические характеристики, принципы построения технических средств передачи и защиты информации, виды сигналов и способы распространения,. ***Уметь:*** Осуществлять	***Знать:*** каналы утечки конфиденциальной информации по техническим каналам, основные тактико-технические характеристики, принципы построения технических средств передачи и защиты информации, виды сигналов и способы распространения, принципы и способы

1	2	3	4	5
		средств защиты информации. ***Владеть:*** навыками фиксации инцидентов, связанных с осуществлением угроз безопасности.	эксплуатацию технических средств защиты информации в соответствии с требованиями инструкций, эксплуатационной документации. ***Владеть:*** навыками прогнозирования рисков, связанных с осуществлением угроз безопасности.	организации системы защиты информации на объектах информатизации. ***Уметь:*** Осуществлять эксплуатацию технических средств защиты информации в соответствии с целями политики информационной безопасности. ***Владеть:*** навыками оценки рисков, связанных с осуществлением угроз безопасности.
	ОПК-9.2.2 Проводить текущий контроль показателей и процесса функционирования телекоммуникационных систем и сетей	***Знать:*** знать номенклатуру регламентных работ по восстановлению работоспособности устройств и программ ***Уметь:*** выполнять этапы регламентных работ по восстановлению работоспособности устройств и программ ***Владеть (или Иметь опыт деятельности):*** эксплуатации программного и аппаратного обеспечения ТКС в основных режимах работы	***Знать:*** знать правила проведения 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 аппаратного обеспечения ТКС в различных режимах работы	***Знать:*** знать порядок осуществления и правила проведения регламентных работ по восстановлению работоспособности устройств и программ ***Уметь:*** выполнять разнообразные работы по восстановлению работоспособности устройств и программ ***Владеть (или Иметь опыт деятельности):*** эксплуатации программного и аппаратного обеспечения ТКС в нетиповых режимах работы
	ОПК-9.2.3 Использует средства измерений	***Знать:*** основные признаки возникновения ошибок в	***Знать:*** характеристики ошибок в телекоммуникацио	***Знать:*** методики обнаружения ошибок в телекоммуникацио

1	2	3	4	5
	и контроля процесса и параметров функционирования телекоммуникационных систем и сетей	телекоммуникационных системах и сетях ***Уметь:*** в процессе эксплуатации фиксировать режимы работы в телекоммуникационных системах и сетях, отличные от штатных ***Владеть (или Иметь опыт деятельности):*** навыками обнаружения сбоев и отказов в в телекоммуникационных системах и сетях	нных системах и сетях ***Уметь:*** в процессе эксплуатации фиксировать и описывать требуемым образом режимы работы в телекоммуникационных системах и сетях, отличные от штатных ***Владеть (или Иметь опыт деятельности):*** навыками обнаружения и устранения сбоев и отказов в в телекоммуникационных системах и сетях	нных системах и сетях ***Уметь:*** в процессе эксплуатации предусматривать режимы работы в телекоммуникационных системах и сетях, отличные от штатных ***Владеть (или Иметь опыт деятельности):*** навыками прогнозирования сбоев и отказов в в телекоммуникационных системах и сетях
ОПК-9.3/ завершающий	ОПК-9.3.1 Использует сканеры безопасности телекоммуникационных систем и сетей	***Знать:*** Профили защиты инструментальных средств обеспечения защиты информации телекоммуникационных систем. ***Уметь:*** настройку средств реализации профилей защиты. ***Владеть:*** Навыками наблюдения за процессом и параметров функционирования телекоммуникационных систем и сетей.	***Знать:*** Порядок использования профилей защиты инструментальные средства обеспечения защиты информации телекоммуникационных систем. ***Уметь:*** Осуществлять внедрение средств реализации профилей защиты. ***Владеть:*** Навыками описания процесса и параметров функционирования телекоммуникационных систем и сетей.	***Знать:*** Методику формирования профилей защиты инструментальные средства обеспечения защиты информации телекоммуникационных систем. ***Уметь:*** Осуществлять рациональный выбор средств реализации профилей защиты. ***Владеть:*** Навыками контроля процесса и параметров функционирования телекоммуникационных систем и сетей.
	ОПК-9.3.2 Применяет методы анализа	***Знать:*** виды инструментальных средств контроля защищенности	***Знать:*** классификацию, виды и типы инструментальных	***Знать:*** классификацию, виды и типы инструментальных

1	2	3	4	5
	защищенности телекоммуникационных систем и сетей	информации в телекоммуникационных системах; ***Уметь:*** применять инструментальные средства контроля защищенности информации в телекоммуникационных системах. ***Владеть:*** навыками инструментального контроля защищенности информации в автоматизированных системах;.	средств контроля защищенности информации в телекоммуникационных системах; ***Уметь:*** применять инструментальные средства контроля защищенности информации в телекоммуникационных системах; производить оценку полученных результатов. ***Владеть:*** навыками инструментального контроля защищенности информации в автоматизированных системах; анализа защищенности телекоммуникационных систем; навыками выбора инструментальных средств контроля защищенности информации;.	средств контроля защищенности информации в телекоммуникационных системах; Методы и способы контроля защищенности информации; ***Уметь:*** применять инструментальные средства контроля защищенности информации в телекоммуникационных системах; производить оценку полученных результатов; сопоставлять результаты измерений с требуемыми значениями. ***Владеть:*** навыками инструментального контроля защищенности информации в автоматизированных системах; анализа защищенности телекоммуникационных систем; навыками выбора инструментальных средств контроля защищенности информации; навыками интерпретации результатов измерений и определения подхода для повышения защищенности телекоммуникационных систем.
	ОПК-9.3.3	***Знать:***	***Знать:***	***Знать:***

1	2	3	4	5
	Проводит настройку средств автоматического реагирования на попытки несанкционированного доступа	номенклатуру средств защищенности телекоммуникационных систем и сетей ***Уметь:*** использовать функциональные возможности компонентов телекоммуникационных систем и сетей ***Владеть (или Иметь опыт деятельности):*** навыками эксплуатации телекоммуникационных систем сетей в основных состояниях	номенклатуру, технические характеристики средств защищенности телекоммуникационных систем и сетей ***Уметь:*** использовать функциональные возможности компонентов телекоммуникационных систем и сетей для повышения защищенности телекоммуникационных систем и сетей ***Владеть (или Иметь опыт деятельности):*** навыками эксплуатации телекоммуникационных систем сетей в различных состояниях	номенклатуру, принципы организации, технические характеристики средств защищенности телекоммуникационных систем и сетей ***Уметь:*** использовать функциональные возможности компонентов телекоммуникационных систем и сетей для анализа защищенности телекоммуникационных систем и сетей ***Владеть (или Иметь опыт деятельности):*** навыками эксплуатации телекоммуникационных систем сетей в нетиповых состояниях

6.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения основной профессиональной образовательной программы

Таблица 6.3 – Контрольные задания и иные материалы для оценки результатов обучения по практике (знаний, умений, навыков и (или) опыта деятельности)

Код компетенции/этап формирования компетенции в процессе освоения ОПОП ВО *(указывается название этапа из п.6.1)*	Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности
ОПК-5	Дневник практики.

завершающий	Отчёт по практике с научно-обоснованными решениями по увеличению защищённости телекоммуникационных систем и сетей Доклад обучающегося на промежуточной аттестации (защита отчета о практике). Характеристика руководителя практики от организации управленческих качеств обучающегося.
ОПК -6 завершающий	Дневник практики. Отчет о практике. Ответы на вопросы по содержанию практики на промежуточной аттестации.
ОПК -9 завершающий	Дневник практики. Отчет о практике. Раздел отчета о практике – *Результаты работы со средствами программно-аппартной защиты информации в ТКС.* Типовое задание № 1 по практической подготовке, предусматривающее выполнение обучающимся вида(ов) работ, связанного(ых) с будущей профессиональной деятельностью (задание конкретизируется с учетом особенностей конкретной профильной организации в Дневнике практики, в п.1.4 задания студенту): *Выполнить настройку программно-аппаратного средства защиты информации в соответствие с заданной политикой информационной безопасности.* Доклад обучающегося на промежуточной аттестации (защита отчета о практике). Характеристика руководителя практики от организации управленческих качеств обучающегося.
ОПК -10 завершающий	Дневник практики. Отчет о практике: Доклад обучающегося на промежуточной аттестации (защита отчета о практике). Характеристика руководителя практики от организации управленческих качеств обучающегося.
ОПК -16 завершающий	Дневник практики. Отчет о практике. Графические материалы к отчету. Доклад обучающегося на промежуточной аттестации (защита отчета о практике). Характеристика руководителя практики от организации управленческих качеств обучающегося.
ОПК -9.1 завершающий	Дневник практики. Типовое задание № 2 по практической подготовке, предусматривающее выполнение обучающимся вида(ов) работ, связанного(ых) с будущей профессиональной деятельностью (задание конкретизируется с учетом особенностей конкретной профильной организации в Дневнике практики, в п.1.4 задания студенту): *Восстановите активность сетевых приложений по предложенному вам журналу брандмауэра.* Графические материалы к отчету. Раздел отчета о практике – *Результаты проведенного мониторинга (и (или) производственного контроля) работоспособности ТКС.* Отчет о практике:

	Доклад обучающегося на промежуточной аттестации (защита отчета о практике). Характеристика руководителя практики от организации управленческих качеств обучающегося.
ОПК -9.2 завершающий	Дневник практики. Отчет о практике. Типовое задание № 3 по практической подготовке, предусматривающее выполнение обучающимся вида(ов) работ, связанного(ых) с будущей профессиональной деятельностью (задание конкретизируется с учетом особенностей конкретной профильной организации в Дневнике практики, в п.1.4 задания студенту): *Реализуйте с помощью средства мониторинга сетевых соединений требуемую политику безопасности.* Доклад обучающегося на промежуточной аттестации (защита отчета о практике). Характеристика руководителя практики от организации управленческих качеств обучающегося.
ОПК -9.3 завершающий	Дневник практики. Графические материалы к отчету. Раздел отчета о практике – *Результаты проведенного мониторинга (и (или) производственного контроля) работоспособности ТКС.* Отчет о практике: Доклад обучающегося на промежуточной аттестации (защита отчета о практике). Характеристика руководителя практики от организации управленческих качеств обучающегося.

6.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Оценка знаний, умений, навыков, характеризующая этапы формирования компетенций, закрепленных за производственной преддипломной 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			