МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

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

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

Производственная преддипломная практика
(наименование вида и типа практики)

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

Безопасность автоматизированных систем
наименование направленности (профиля, специализации)

в сфере информационных и коммуникационных технологий

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

Курск – 2021

Рабочая программа практики составлена в соответствии с:

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

– ОПОП ВО 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий», одобренным Ученым советом университета (протокол № 6 «22» февраля 2021г.).

Рабочая программа практики обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий» на заседании кафедры информационной безопасности «30» августа 2021 г., протокол № 1.

Зав. кафедрой _____ Таныгин М.О.

Разработчик программы

к.т.н., доцент _____ Таныгин М.О.

(ученая степень и ученое звание, Ф.И.О.)

Директор научной библиотеки _____ Макаровская В.Г.

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

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа практики пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.03.01 Информационная безопасность на основании учебного плана ОПОП ВО 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий», одобренного Ученым советом университета протокол №__«___» _____ 20 ___ г., на заседании кафедры_____.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

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

1.1. Цель практики

Целью производственной преддипломной практики является получение профессиональных умений и опыта профессиональной деятельности в области информационной безопасности в условиях реального производства.

1.2. Задачи практики

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

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

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

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

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

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

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

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

Таблица 2 – Результаты обучения по практике

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за практикой)		*Код и наименование индикатора достижения компетенции, закрепленного за практикой*	*Планируемые результаты обучения по практике, соотнесенные с индикаторами достижения компетенций*
код	*наим*		
УК-1	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1 Анализирует задачу, выделяя ее базовые составляющие	***Знать:*** - основные этапы развития технологии программирования; - принципы построения программных систем ***Уметь:*** - пользоваться понятийным аппаратом методов разработки программных систем; - анализировать предметную область и создавать декларативное описание задачи; - применять принципы функционирования программных систем; - выполнять операции импорта/экспорта данных при работе с программными средами. ***Владеть (****или* ***Иметь опыт деятельности):*** - базовыми элементами технологии разработки; - программными приемами декларативного описания предметной области; - навыками структуризации знаний и его программирования.
		УК-1.2 Определяет и ранжирует информацию, требуемую для решения поставленной задачи	***Знать:*** - этапы разработки программного обеспечения; - модели жизненного цикла программного обеспечения; ***Уметь:*** **-** разрабатывать техническое задание на проектирование программного обеспечения; - принимать обоснованные решения по выбору архитектуры программного обеспечения, среды программирования, стандартов разработки; ***Владеть (****или* ***Иметь опыт деятельности):*** - правилами ранжирования информации; - процедурами упорядочения элементов.
		УК-1.3 Осуществляет поиск информации для	***Знать:*** - методы повышения уровня защищенности информационных систем;

		решения поставленной задачи по различным типам запросов	**-** стандарты, предназначенные для контроля качества процессов защиты исследуемого объекта - нормативно-правовые аспекты обеспечения информационной безопасности. ***Уметь:*** - формализовать сведения для запросов; - выбирать тип запроса; - составлять простые и составные запросы. ***Владеть (****или* ***Иметь опыт деятельности):*** **-** общими приемами организации поиска; - алгоритмическими схемами стратегий поиска; - навыками программирования поисковых процедур.
		УК-1.4 При обработке информации отличает факты от мнений, интерпретаций, оценок, формирует собственные мнения и суждения, аргументирует свои выводы, в том числе с применением философского понятийного аппарата	***Знать:*** - требования, предъявляемые к гипотезам научного исследования - виды гипотез; - основные методы классификации и оценки информационных ресурсов; - основные положения, теоретические принципы и методологические принципы логики. ***Уметь:*** - формулировать и аргументировано отстаивать собственную позицию по различным проблемам информационной безопасности; - использовать первоисточники в процессе научного исследования; - уметь логически мыслить, вести научные дискуссии; - применять навыки самостоятельной работы и развития своих творческих способностей и логического мышления. ***Владеть (****или* ***Иметь опыт деятельности):*** **-** навыками восприятия и анализа текстов, имеющих философское содержание; - навыками ведения дискуссии и полемики; - навыками выражения и обоснования собственной позиции относительно философских позиций.
		УК-1.5 Анализирует пути решения проблем мировоззренческого, нравственного и личностного характера на основе использования основных философских идей и категорий в их историческом развитии и социально-культурном контексте	***Знать:*** - требования, предъявляемые к гипотезам научного исследования - виды гипотез; - основные методы классификации и оценки информационных ресурсов; - основные положения, теоретические принципы и методологические принципы логики. ***Уметь:*** - анализировать пути решения проблем мировоззренческого, нравственного и личностного характера на основе использования основных философских идей и категорий; - использовать положения и категории философии для оценивания и анализа различных социальных тенденций, фактов и явлений; - использовать первоисточники в процессе научного исследования;

			- применять навыки самостоятельной работы и развития своих творческих способностей и логического мышления. ***Владеть (****или* ***Иметь опыт деятельности):*** **-** навыками восприятия и анализа текстов, имеющих философское содержание; - навыками ведения дискуссии и полемики; - навыками аналитической оценки социально-гуманитарного материала;
ПК-4	Способен выполнять работы по проектированию автоматизированных систем в защищенном исполнении	ПК-4.1 Разрабатывает проектные документы на средства защиты информации создаваемых автоматизированных систем	***Знать:*** - методы проектирования и построения систем информационной безопасности, включая методы тестирования эффективности и оценки надёжности; - основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, в области управления информационной безопасностью с целью разработки проектов организационно-распорядительных документов; - основные нормативные правовые акты в области обеспечения информационной безопасности. ***Уметь:*** - уметь проводить выбор, исследовать эффективность, проводить технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности; - уметь разрабатывать технические задания на создание подсистем обеспечения информационной безопасности; - разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации. ***Владеть (или Иметь опыт деятельности):*** - навыками разработки политик безопасности различных уровней; - правилами построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, стоимости и сроков реализации; - навыками работы с нормативными правовыми актами в области информационной безопасности.
		ПК-4.2 Готовит техническую и проектную документацию по вопросам создания и эксплуатации автоматизированных систем	***Знать:*** -основные нормативно-правовые акты в области информационной безопасности и защиты информации; - правовые основы организации защиты государственной тайны и конфиденциальной информации; - основные методы организации и проведения технического обслуживания вычислительной техники и других технических средств ин-

			форматизации. ***Уметь:*** **- о**формлять техническую и проектную документацию по регламентации вопросов создания и эксплуатации автоматизированных систем; - оформлять техническую документацию в соответствии с действующими нормативными документами. ***Владеть (****или* ***Иметь опыт деятельности):*** ***- навыками в***едения документов учета, обработки, хранения и передачи информации, составляющей профессиональную, коммерческую, служебную или иную тайну.
		ПК-4.3 Проверяет программы и алгоритмы на предмет соответствия требованиям защиты информации	***Знать:*** - требования защиты информации; -методы повышения уровня защищенности информационных систем; **-** стандарты, предназначенные для контроля функциональных характеристик работы системы; ***Уметь:*** - формализовать выборки для формирования сообщений; - составлять простые и составные запросы к системам учета. - проводить анализ основных характеристик системы. ***Владеть (****или* ***Иметь опыт деятельности):*** **-** общими приемами организации поиска; - алгоритмическими схемами оценки характеристик; - навыками анализа ожидаемых и фактических результатов работы системы.
		ПК-4.4 Проводит сравнительный анализ вариантов конфигураций и состава автоматизированных систем	***Знать:*** - основные методы управления защитой информации; - основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; - основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические) - Методы защиты информации в автоматизированных системах - варианты конфигураций и их характеристики. ***Уметь:*** - оценивать информационные риски в автоматизированных системах; - классифицировать и оценивать угрозы безопасности информации; - определять подлежащие защите информационные ресурсы автоматизированных систем; -разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем; - конфигурировать параметры системы защиты информации автоматизированных систем. ***Владеть (****или* ***Иметь опыт деятельности):***

			- навыками проведения сравнительного анализа; - навыками проведения различных конфигураций; - навыками разработки предложений по совершенствованию систем защиты информации.
ПК-5	Способен выполнять работы по обеспечению информационной безопасности автоматизированных систем на всех этапах их жизненного цикла	ПК-5.1 Проверяет соответствие внедряемых решений и средств для обеспечения информационной безопасности требованиям реализуемой политики безопасности	***Знать****:* - - реализуемую политику безопасности; - основные характеристики программных и технических средств разработки ПО; - особенности проверки внедряемых решений и средств для обеспечения информационной безопасности; ***Уметь****:* - строить модели формирования решений для обеспечения информационной безопасности; -находить возможные решения и средства информационной безопасности; - анализировать возможные несоответствия внедряемых решений. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыком выбора соответствующего решения/ средства для обеспечения информационной безопасности; - навыками разработки средств обеспечения информационной безопасности; - навыками определения соответствия выбранных средств реализуемой политики безопасности.
		ПК-5.2 Восстанавливает работоспособность автоматизированных систем после инцидентов информационной безопасности	***Знать:*** - особенности автоматизированных систем; - виды инцидентов информационной безопасности; - особенности восстановления автоматизированных систем после инцидентов информационной безопасности. ***Уметь:*** - определять причину возникновения инцидента информационной безопасности; - анализировать предметную область и создавать декларативное описание задачи; - применять принципы выявления ключевых параметров работы автоматизированной системы; ***Владеть (****или* ***Иметь опыт деятельности):*** - приемами анализа полноты и корректности ключевых параметров эксплуатации автоматизированных систем; - навыком определения вида инцидента; - навыком восстановления работоспособности автоматизированной системы.
		ПК-5.3 Проводит операции вывода защищённых автоматизированных систем из эксплуатации	***Знать:*** - содержание и порядок выполнения работ на стадиях создания автоматизированных систем в защищенном исполнении; - технологии повышения защищенности автоматизированных систем из эксплуатации; - особенности вывода защищённых автоматизированных систем из эксплуатации.

			Уметь: - выполнять определять характер угрозы и масштабы последствий; - проектировать регламент защищенного взаимодействия компонентов автоматизированных систем; - минимизировать последствия ущерба за счет интеграции средств защиты. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками разработки компонентов автоматизированных систем; - навыками обеспечения совместимого взаимодействия отдельных модулей; - навыками вывода защищённых автоматизированных систем из эксплуатации.
ПК-7	Способен определять уровень защищённости автоматизированных систем	ПК-7.1 Формулирует целевые показатели функционирования защищенных автоматизированных систем	***Знать:*** - критерии оценки защищенности автоматизированной системы; - регламент информирования персонала автоматизированной системы о выявленных инцидентах; - регламент учета выявленных инцидентов; - основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации в автоматизированных системах. ***Уметь:*** - определять источники и причины возникновения инцидентов; - формулировать целевые показатели функционирования защищённых автоматизированных систем; - проводить оценку защищенности автоматизированных систем с помощью типовых программных средств; - рассчитывать и проводить инструментальный контроль показателей эффективности защиты информации; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками определения источников и причин возникновения инцидентов; - навыками расчёта целевых показателей защищённых автоматизированных систем.
		ПК-7.2 Анализирует уязвимости автоматизированных систем в соответствии с нормативными документами	***Знать:*** - нормативные документы; - особенности анализа уязвимости автоматизированные систем; - основные виды уязвимости автоматизированных систем. ***Уметь:*** - анализировать уязвимости автоматизированных систем в соответствии с требованиями; - минимизировать количество потенциальных несоответствий. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками установки директив, определяющих работу автоматизированных систем; - навыками проведения анализа нормативных документов; - технологией ведения протокола работы си-

			стемы с выводом промежуточных результатов обработки данных.
		ПК-7.3 Формулирует угрозы информационной безопасности исходя из выявленных характеристик автоматизированной системы	***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.
ПК-8	Способен выполнять задачи по выявлению уязвимых узлов автоматизированной системы	ПК-8.1 Разрабатывает методическую, техническую, рекомендательную и отчётную документацию по анализу защищённости автоматизированной системы	***Знать:*** - содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации; - основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; - основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах; нормативно-правовые акты в области информационной безопасности и защиты информации. ***Уметь:*** - анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации - разрабатывать методическую, техническую, рекомендательную и отчётную документацию по анализу защищённости автоматизированной системы; - контролировать эффективность принятых мер по защите информации в автоматизированных системах. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками анализ компонентов автоматизированных систем; - навыками разработки документации.
		ПК-8.2 Осуществляет подбор программных средств тестирования защищённости автоматизированной системы в зависимости от предъяв-	***Знать:*** - принципы построения и функционирования систем и сетей передачи информации; - основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; - основные меры по защите информации в

		ляемым к ней требованиям	автоматизированных системах - принципы построения средств защиты информации от утечки по техническим каналам; - основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах; - технические каналы утечки информации; - технические средства контроля эффективности мер защиты информации ***Уметь :*** - анализировать основные узлы и устройства современных автоматизированных систем; - применять действующую нормативную базу в области обеспечения безопасности информации; - контролировать безотказное функционирование технических средств защиты информации - составлять методики тестирования систем защиты информации автоматизированных систем - подбирать программные средства тестирования систем защиты информации автоматизированных систем. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками установки программных средств защиты; - навыками оценки защищенности информационной системы с учетом возможных угроз. - навыками анализа основных узлов и устройств современных автоматизированных систем.
		ПК-8.3 Использует средств инструментального анализа защищённости программных и аппаратных платформ узлов автоматизированной системы	***Знать:*** - принципы построения компьютерных систем и сетей; - формальные модели безопасности компьютерных систем и сетей; - принципы построения систем обнаружения компьютерных атак; - методы обработки данных мониторинга безопасности компьютерных систем и сетей; - порядок создания и структура отчета, создаваемого по результатам проверок; - способы обнаружения и нейтрализации последствий вторжений в компьютерные системы; - криптографические протоколы.. ***Уметь:*** - формализовывать задачу управления безопасностью автоматизированных систем; - применять инструментальные средства проведения мониторинга защищенности автоматизированных систем; - применять методы анализа защищенности компьютерных систем и сетей; - структурировать аналитическую информацию для включения в отчет. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками выполнения анализа защищенности; - навыками составления отчетов по результатам проверок

		ПК-8.4 Проводит контроль защищённости и функционирования программно-аппаратных и технических средств автоматизированной системы	***Знать:*** **-** основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности информации; - способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; -принципы построения систем защиты информации. ***Уметь:*** - классифицировать и оценивать угрозы безопасности информации для объекта информатизации; -разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем; - разрабатывать политики безопасности информации автоматизированных систем; - применять действующую законодательную базу в области обеспечения защиты информации ***Владеть (или Иметь опыт деятельности):*** - навыками оценки информационных рисков; - навыками экспертизы состояния защищенности информации автоматизированных систем; - навыками обоснования критериев эффективности функционирования защищенных автоматизированных систем.
ПК -9	Способен организовывать работы по обеспечению информационной безопасности в автоматизированных системах	ПК-9.1 Формулирование правил работы персонала со средствами защиты информации	***Знать:*** **-** Нормативно-правовые акты в области информационной безопасности и защиты информации; **-** регламент информирования персонала автоматизированной системы о выявленных инцидентах ***Уметь:*** - устанавливать и настраивать средства защиты информации; - Выявлять степень участия персонала в обработке защищаемой информации; - осуществлять планирование и организацию работы персонала автоматизированной системы с учетом требований по защите информации; - обучать персонал автоматизированной системы комплексу мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения защиты информации. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками оценки работы технических средств; - навыками анализа эффективности их работы; - навыками разработки регламентов работы.
ПК-10	Способен собирать, анализировать и систематизировать информацию по за-	ПК-10.1 Соотносит инциденты информационной безопасности с характеристиками систем и	***Знать:*** **-** типовые инциденты информационной безопасности АС, состав, документацию, характеристики и принцип работы оборудования

	фиксированным инцидентам информационной безопасности	средств защиты информации	АС; - классификацию, состав, документацию, способы применения систем и средств защиты информации в АС. ***Уметь:*** **-** классифицировать инциденты информационной безопасности АС; - применять средства защиты информации в АС; - определять уязвимые узлы в системе информационной безопасности; - осуществлять контроль функционирования систем и средств защиты АС; - проводить анализ результатов выполняемых работ. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками применения программных и аппаратных средств защиты информации в АС; - обнаружения инцидентов и восстановления функционирования оборудования АС; - контроля и анализа результатов выполняемых работ.
		ПК-10.4 Формулирует правила протоколирования результатов мониторинга безопасности автоматизированных систем	***Знать:*** **-** задачи и функции систем и средств мониторинга и управления средствами обеспечения безопасности АС; - правила эксплуатации оборудования и программных средств управления средствами защиты АС; - классификацию и способы применения средств и систем защиты АС. ***Уметь:*** **-** проводить анализ защищенности АС; - разрабатывать правила протоколирования результатов мониторинга АС; - настраивать оборудования и программных средств мониторинга и управления средствами защиты АС; - средства и системы защиты АС. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками анализа защищенности АС; - навыками эксплуатации программных средств мониторинга и управления средствами зашиты АС; - навыками разработки правил протоколирования результатов мониторинга АС; - навыками настройки оборудования и программных средств мониторинга и управления средствами защиты АС.

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

Производственная технологическая практика входит в часть, формируемую участниками образовательных отношений блока 2 «Практика» основной профессиональной образовательной программы – программы бакалавриата ОПОП ВО 10.03.01 Информационная безопасность на основании учебного плана ОПОП ВО 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий»,. Практика проходит на 4 курсе в 8 семестре.

Объем производственной преддипломной практики, установленный учебным планом, – 9 зачетных единиц, продолжительность – 4 недели (216 часов).

4 Содержание практики

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

Контактная работа по практике (включая контактную работу по промежуточной аттестации по практике) составляет 4 часа, работа обучающегося в иных формах – 212 часов.

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

Таблица 4 – Этапы и содержание практики

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

2	Основной этап	Работа обучающихся в профильной организации	174
2.1	Знакомство с профильной организацией	Знакомство с профильной организацией, руководителем практики от организации, рабочим местом и должностной инструкцией.	2
		Инструктаж по технике безопасности на рабочем месте.	2
		Знакомство с содержанием деятельности профильной организации по обеспечению информационной безопасности и проводимыми в нем мероприятиями.	
		Изучение нормативных правовых актов профильной организации по обеспечению информационной безопасности (политика безопасности профильной организации, положения, приказы, инструкции, должностные обязанности, памятки и др.).	1
2.2	Практическая подготовка обучающихся *(непосредственное выполнение обучающимися видов работ, связанных с будущей профессиональной деятельностью)*	Самостоятельное проведение мониторинга и (или) производственного контроля эффективности применения средств защиты информации в ТКС. Организация работы 2-3 человек и руководство их работой в процессе проведения мониторинга безопасности ТКС. Создание плана работы коллектива из 3 – 4 человек, реализующего политику безопасности в ТКС	144.

		Самостоятельная обработка и систематизация полученных данных с помощью профессиональных программных комплексов и информационных технологий. *Организация работы 2-3 человек и руководство их работой в процессе обработки и систематизации полученных данных.* Представление результатов мониторинга руководителю практики от организации	
		Самостоятельное проведение анализа результатов проведенного мониторинга информационной безопасности. Организация работы 2-3 человек и руководство их работой в процессе работ по обеспечению информационной безопасности. Оценка рисков информационной безопасности. Представление результатов анализа и обоснование оценки руководителю практики от организации.	
		Самостоятельная подготовка рекомендаций по повышению уровня информационной безопасности предприятия. *Организация работы 2-3 человек и руководство их работой в процессе подготовки рекомендаций по повышению уровня информационной безопасности предприятия.* Представление своих рекомендаций руководителю практики от организации.	
		Самостоятельное составление краткосрочного плана работ по обеспечению безопасности организации, эксплуатирующей ТКС. *Организация работы 2-3 человек*	

		и руководство их работой в процессе составления краткосрочного и долгосрочного прогнозов. Представление своего прогноза с обоснованием руководителю практики от организации.	
3	Заключительный этап	Оформление дневника практики.	36
		Составление отчета о практике.	
		Подготовка графических материалов для отчета.	
		Представление дневника практики и защита отчета о практике на промежуточной аттестации.	

5 Указание форм отчетности по практике

Формы отчетности студентов о прохождении производственной производственной практики:

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

– отчет о практике.

Структура отчета о производственной преддипломной практике:

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

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

– Основные нормативные правовые акты предприятия по обеспечению информационной безопасности.

– Анализ результатов мониторинга.

– Оценка рисков информационной безопасности ТКС.

– Рекомендации по повышению уровня информационной безопасности предприятия.

– Краткосрочный и долгосрочный прогноз развития ситуации.

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

Отчет должен быть оформлен в соответствии с:

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

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

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

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

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

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

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

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

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

6 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по практике

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

Таблица 6.1 – Этапы формирования компетенций

Код и наименование компетенции	Этапы* формирования компетенций и дисциплины (модули), практики, НИР, при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
УК-1	Основы информационной безопасности Философия	Безопасность систем баз данных	Сети и системы передачи информации Производственная преддипломная практика
ПК-4	Проектирование защищенных автоматизированных систем	Методы защиты программного обеспечения	Производственная преддипломная практика
ПК-5	Комплексная защита объектов информатизации Методы защиты программного обеспечения		Производственная преддипломная практика

ПК-7	Комплексная защита объектов информатизации		Производственная преддипломная практика
ПК-8	Комплексная защита объектов информатизации		Производственная преддипломная практика
ПК-9	Системы охраны и инженерной защиты информации	Организация и управление службой защиты информации Работа с конфиденциальной информацией	Экономика защиты информации Оценка рисков информационной безопасности Производственная преддипломная практика
ПК-9	Экономика защиты информации Оценка рисков информационной безопасности		Производственная преддипломная практика

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

Таблица 6.2 – Показатели и критерии оценивания компетенций, шкала оценивания

Код компетенции/ этап *(указывается название этапа из п.6.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за практикой)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
ПК-1/ завершающий	УК-1.1 Анализирует задачу, выделяя ее базовые составляющие	***Знать:*** - основные этапы организации защиты информационных систем; ***Уметь:*** - пользоваться понятийным аппаратом информационных технологий; - анализировать предметную область и создавать декларативное описание задачи; ***Владеть (или Иметь опыт деятельности):***	***Знать:*** - основные этапы организации защиты информационных систем; - принципы оценки информационной безопасности ***Уметь:*** - пользоваться понятийным аппаратом информационных технологий; - анализировать предметную область и создавать декларативное описание задачи;	***Знать:*** - основные этапы организации защиты информационных систем; - принципы оценки информационной безопасности ***Уметь:*** - пользоваться понятийным аппаратом информационных технологий; - анализировать предметную область и создавать декларативное описание задачи;

1	2	3	4	5
		- приемами декларативного описания предметной области;	- применять принципы выявления ключевых параметров работы информационной системы; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками структуризации знаний и его формализации.	- применять принципы выявления ключевых параметров работы информационной системы; - выполнять операции импорта/экспорта данных при работе с программными средами. ***Владеть (****или* ***Иметь опыт деятельности):*** - приемами декларативного описания предметной области; - навыками структуризации знаний и его формализации.
	УК-1.2 Определяет и ранжирует информацию, требуемую для решения поставленной задачи	***Знать:*** - модели жизненного цикла программного обеспечения; ***Уметь:*** - разрабатывать техническое задание на проектирование программного обеспечения; ***Владеть (****или* ***Иметь опыт деятельности):*** - правилами ранжирования информации;	***Знать:*** - этапы разработки программного обеспечения; ***Уметь:*** - принимать обоснованные решения по выбору архитектуры программного обеспечения, среды программирования, стандартов разработки; ***Владеть (****или* ***Иметь опыт деятельности):*** - правилами ранжирования информации; - процедурами упорядочения элементов.	***Знать:*** - этапы разработки программного обеспечения; - модели жизненного цикла программного обеспечения; ***Уметь:*** - разрабатывать техническое задание на проектирование программного обеспечения; - принимать обоснованные решения по выбору архитектуры программного обеспечения, среды программирования, стандартов разработки; ***Владеть (****или* ***Иметь опыт деятельности):*** - правилами ранжирования информации;

1	2	3	4	5
				- процедурами упорядочения элементов.
	УК-1.3 Осуществляет поиск информации для решения поставленной задачи по различным типам запросов	***Знать:*** - методы повышения уровня защищенности информационных систем; ***Уметь:*** - формализовать сведения для запросов; - выбирать тип запроса; ***Владеть (****или* ***Иметь опыт деятельности):*** - общими приемами организации поиска; - алгоритмическими схемами стратегий поиска;	***Знать:*** - методы повышения уровня защищенности информационных систем; - стандарты, предназначенные для контроля качества процессов защиты исследуемого объекта ***Уметь:*** - формализовать сведения для запросов; - составлять простые и составные запросы. ***Владеть (****или* ***Иметь опыт деятельности):*** - общими приемами организации поиска; - навыками программирования поисковых процедур.	***Знать:*** - методы повышения уровня защищенности информационных систем; - стандарты, предназначенные для контроля качества процессов защиты исследуемого объекта - нормативно-правовые аспекты обеспечения информационной безопасности. ***Уметь:*** - формализовать сведения для запросов; - выбирать тип запроса; - составлять простые и составные запросы. ***Владеть (****или* ***Иметь опыт деятельности):*** - общими приемами организации поиска; - алгоритмическими схемами стратегий поиска; - навыками программирования поисковых процедур.
	УК-1.4 При обработке информации отличает факты от мнений, интерпретаций, оценок, формирует собственные	***Знать***: структуру способа творческой деятельности; факторы, определяющие круг профессиональных обязанностей и их состав; принципы планирования массовых информационных	***Знать***: Российские и международные этические нормы, кодексы профессиональной этики; понимать значение этических регуляторов в деятельности. социально-психологические	***Знать***: понимать значение этических регуляторов в деятельности. социально-психологические характеристики больших групп; структуру и функции общения, особенности внутриг-

1	2	3	4	5
	мнения и суждения, аргументирует свои выводы, в том числе с применением философского понятийного аппарата	потоков, виды планов; характер организаторской работы; основные источники информации; причины, вызывающие жанровую дифференциацию творчества. ***Уметь***: грамотно и профессионально проанализировать конкретный материал; составить заявку на тему своего выступления; спланировать творческий акт в целом и его отдельные операции; предпринимать необходимые профессиональные действия для осуществления организаторской деятельности; охарактеризовать основные жанровые модели текстов и основные технологии творчества в том или ином жанре; проанализировать жанровый состав материалов предлагаемого номера и конкретный материал определенного жанра; ***Владеть***: навыками реализации профессионально-творческих замыслов и редакционных планов по непосредственному созданию материалов различных жанров для их публикации; составле-	характеристики больших групп; структуру и функции общения, особенности внутригруппового общения; основные социально-психологические теории; основные процессы динамики малых групп; социально-психологические характеристики личности и механизмы их формирования; ***Уметь:*** проанализировать жанровый состав материалов предлагаемого номера и конкретный материал определенного жанра; ***Владеть***: навыками реализации профессионально-творческих замыслов и редакционных планов по непосредственному созданию материалов различных жанров для их публикации; составления долгосрочных и краткосрочных планов; применения необходимых методов творческой деятельности; анализа текстов; редакторской работы; работы с техническими средствами деятельности.	руппового общения; основные социально-психологические теории; основные процессы динамики малых групп; социально-психологические характеристики личности и механизмы их формирования; основные закономерности межгруппового взаимодействия; социальный смысл участия общества в коммуникации; быть осведомленным относительно направлений, содержания и методов теоретических и эмпирических исследований; ***Уметь***: интерпретировать социально-психологические явления с позиции теоретических подходов; выбирать валидные средства диагностики и коррекции социально-психологических феноменов; ***Владеть***: навыками этического анализа профессиональных действий навыками формирования заказа на проведение исследований специальными центрами, а также (в рамках имеющихся возможностей) организации необхо-

1	2	3	4	5
		ния долгосрочных и краткосрочных планов;		димых редакционных исследований.
	УК-1.5 Анализирует пути решения проблем мировоззренческого, нравственного и личностного характера на основе использования основных философских идей и категорий в их историческом развитии и социально-культурном контексте	***Знать***: - современные научно-технические проблемы глобального мира ***Уметь***: - подобрать необходимые источники для устного выступления и презентации ***Владеть***: - категориально-понятийным аппаратом	***Знать***: - основные характеристики структурных элементов научного знания ***Уметь***: - анализировать внутреннюю логику развития научного знания, используя современные представления о динамике науки ***Владеть:*** - навыками критического анализа	***Знать***: - историко-философские концепции о науке и технике ***Уметь***: - использовать эвристические, этические и теоретико-методологические ресурсы философии науки в собственных научных исследованиях ***Владеть***: - навыками самоанализа и самооценки
ПК-4/ завершающий	ПК-4.1 Разрабатывает проектные документы на средства защиты информации создаваемых автоматизированных систем	***Знать:*** номенклатуру правил выполнения работ по обеспечению информационной безопасности ***Уметь:*** с недостатками документально описывать применяемые для обеспечения безопасности автоматизированных системах технологии ***Владеть (****или* ***Иметь опыт деятельности):*** проведения работ по разработке и модернизации систем защиты информации	***Знать:*** основные правила выполнения работ по обеспечению информационной безопасности ***Уметь:*** документально описывать основные применяемые для обеспечения безопасности автоматизированных системах технологии ***Владеть (****или* ***Иметь опыт деятельности):*** разработки и модернизации систем защиты информации	***Знать:*** правила, регламенты и порядок выполнения работ по обеспечению информационной безопасности ***Уметь:*** документально и в полном объёме описывать применяемые для обеспечения безопасности автоматизированных системах технологии ***Владеть (****или* ***Иметь опыт деятельности):*** разработки и модернизации систем защиты информации для достижения целевых показателей функционирования
	ПК-4.2 Готовит тех-	***Знать:*** номенклатуру этапов жиз-	***Знать:*** основные этапы жизненного	***Знать:*** все возможные этапы

1	2	3	4	5
	ническую и проектную документацию по вопросам создания и эксплуатации автоматизированных систем	ненного цикла автоматизированных систем и регламентные мероприятия на каждом из них ***Уметь:*** выполнять отдельные действия по обеспечению информационной безопасности автоматизированных систем ***Владеть (****или* ***Иметь опыт деятельности):*** систематизации отдельных действий по обеспечению информационной безопасности автоматизированных систем	цикла автоматизированных систем и регламентные мероприятия на каждом из них ***Уметь:*** выполнять небольшие последовательности отдельных действий по обеспечению информационной безопасности автоматизированных систем ***Владеть (****или* ***Иметь опыт деятельности):*** систематизации последовательности действий по обеспечению информационной безопасности автоматизированных систем	жизненного цикла автоматизированных систем и регламентные мероприятия на каждом из них ***Уметь:*** выполнять связанные последовательности действий по обеспечению информационной безопасности автоматизированных систем ***Владеть (****или* ***Иметь опыт деятельности):*** систематизации сложных последовательностей действий по обеспечению информационной безопасности телекоммуникационных систем
	ПК-4.3 Проверяет программы и алгоритмы на предмет соответствия требованиям защиты информации	***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 ин-	***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 уста-	***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
		формационной системы с учетом возможных угроз.	новки программных средств защиты;	программном уровне. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками установки программных средств защиты; - навыками оценки защищенности информационной системы с учетом возможных угроз.
	ПК-4.4 Проводит сравнительный анализ вариантов конфигураций и состава автоматизированных систем	***Знать:*** - основы использования управляющих директив. ***Уметь:*** - минимизировать количество потенциальных нештатных ситуаций работы программы. ***Владеть (****или* ***Иметь опыт деятельности):*** - технологией ведения протокола работы системы с выводом промежуточных результатов обработки данных.	***Знать:*** - особенности вывода промежуточных значений в ходе работы модулей; ***Уметь:*** - минимизировать количество потенциальных нештатных ситуаций работы программы. ***Владеть (****или* ***Иметь опыт деятельности):*** - установки директив, определяющих работу программных модулей;	***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.
ПК-5/ завершающий	ПК-5.1 Проверяет соответ-	**Знать**: - основные характеристики про-	**Знать**: - реализуемую политику безопасно-	**Знать**: - реализуемую политику безопасно-

1	2	3	4	5
	ствие внедряемых решений и средств для обеспечения информационной безопасности требованиям реализуемой политики безопасности	граммных и технических средств разработки ПО; **Уметь**: - строить модели формирования решений для обеспечения информационной безопасности; - анализировать возможные несоответствия внедряемых решений. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками разработки средств обеспечения информационной безопасности; - навыками определения соответствия выбранных средств реализуемой политики безопасности.	сти; - особенности проверки внедряемых решений и средств для обеспечения информационной безопасности; **Уметь**: -находить возможные решения и средства информационной безопасности; - анализировать возможные несоответствия внедряемых решений. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыком выбора соответствующего решения/ средства для обеспечения информационной безопасности; - навыками определения соответствия выбранных средств реализуемой политики безопасности.	сти; - основные характеристики программных и технических средств разработки ПО; - особенности проверки внедряемых решений и средств для обеспечения информационной безопасности; **Уметь**: - строить модели формирования решений для обеспечения информационной безопасности; -находить возможные решения и средства информационной безопасности; - анализировать возможные несоответствия внедряемых решений. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыком выбора соответствующего решения/ средства для обеспечения информационной безопасности; - навыками разработки средств обеспечения информационной безопасности; - навыками определения соответствия выбранных средств реализуемой политики безопасности.
	ПК-5.2 Восстанавливает работо-	***Знать:*** - особенности автоматизированных	***Знать:*** - виды инцидентов информационной	***Знать:*** - особенности автоматизированных

1	2	3	4	5
	способность автоматизированных систем после инцидентов информационной безопасности	систем; - виды инцидентов информационной безопасности; ***Уметь:*** - определять причину возникновения инцидента информационной безопасности; - применять принципы выявления ключевых параметров работы автоматизированной системы; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыком определения вида инцидента; - навыком восстановления работоспособности автоматизированной системы.	безопасности; - особенности восстановления автоматизированных систем после инцидентов информационной безопасности. ***Уметь:*** - анализировать предметную область и создавать декларативное описание задачи; - применять принципы выявления ключевых параметров работы автоматизированной системы; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыком определения вида инцидента; - навыком восстановления работоспособности автоматизированной системы.	систем; - виды инцидентов информационной безопасности; - особенности восстановления автоматизированных систем после инцидентов информационной безопасности. ***Уметь:*** - определять причину возникновения инцидента информационной безопасности; - анализировать предметную область и создавать декларативное описание задачи; - применять принципы выявления ключевых параметров работы автоматизированной системы; ***Владеть (****или* ***Иметь опыт деятельности):*** - приемами анализа полноты и корректности ключевых параметров эксплуатации автоматизированных систем; - навыком определения вида инцидента; - навыком восстановления работоспособности автоматизированной системы.
	ПК-5.3 Проводит операции вывода защищённых	***Знать:*** - содержание и порядок выполнения работ на стадиях создания автомати-	***Знать:*** - технологии повышения защищенности автоматизированных си-	***Знать:*** - содержание и порядок выполнения работ на стадиях создания автомати-

1	2	3	4	5
	автоматизированных систем из эксплуатации	зированных систем в защищенном исполнении; - особенности вывода защищённых автоматизированных систем из эксплуатации. ***Уметь:*** - минимизировать последствия ущерба за счет интеграции средств защиты. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками обеспечения совместимого взаимодействия отдельных модулей; - навыками вывода защищённых автоматизированных систем из эксплуатации.	стем из эксплуатации; - особенности вывода защищённых автоматизированных систем из эксплуатации. ***Уметь:*** - выполнять определять характер угрозы и масштабы последствий; - проектировать регламент защищенного взаимодействия компонентов автоматизированных систем; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками разработки компонентов автоматизированных систем; - навыками вывода защищённых автоматизированных систем из эксплуатации.	зированных систем в защищенном исполнении; - технологии повышения защищенности автоматизированных систем из эксплуатации; - особенности вывода защищённых автоматизированных систем из эксплуатации. ***Уметь:*** - выполнять определять характер угрозы и масштабы последствий; - проектировать регламент защищенного взаимодействия компонентов автоматизированных систем; - минимизировать последствия ущерба за счет интеграции средств защиты. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками разработки компонентов автоматизированных систем; - навыками обеспечения совместимого взаимодействия отдельных модулей; - навыками вывода защищённых автоматизированных систем из эксплуатации.
ПК-7 / основной	ПК-7.1 Формулирует целе-	***Знать:*** перечень реализуемых телекоммуникационной	***Знать:*** структуру реализуемых телекоммуникационной	***Знать:*** структуру и особенности реализуемых телекомму-

1	2	3	4	5
	вые показатели функционирования защищенных автоматизированных систем	системой технологий для удовлетворения требований по информационной безопасности ***Уметь:*** соотносить отдельные технологии информационной безопасности существующим в ТКС уязвимостям ***Владеть (****или* ***Иметь опыт деятельности):*** реализации базовых технологий информационной безопасности	системой технологий для удовлетворения требований по информационной безопасности ***Уметь:*** соотносить основные технологии информационной безопасности существующим в ТКС уязвимостям ***Владеть (****или* ***Иметь опыт деятельности):*** реализации основных технологий информационной безопасности	никационной системой технологий для удовлетворения требований по информационной безопасности ***Уметь:*** соотносить технологии информационной безопасности существующим в ТКС уязвимостям ***Владеть (****или* ***Иметь опыт деятельности):*** реализации стека технологий информационной безопасности
	ПК-7.2 Анализирует уязвимости автоматизированных систем в соответствии с нормативными документами	***Знать:*** - нормативные документы; - основные виды уязвимости автоматизированных систем. ***Уметь:*** - минимизировать количество потенциальных несоответствий. ***Владеть (****или* ***Иметь опыт деятельности):*** - технологией ведения протокола работы системы с выводом промежуточных результатов обработки данных.	***Знать:*** - особенности анализа уязвимости автоматизированные систем; - основные виды уязвимости автоматизированных систем. ***Уметь:*** - анализировать уязвимости автоматизированных систем в соответствии с требованиями; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками установки директив, определяющих работу автоматизированных систем; - технологией ведения протокола работы системы с выводом промежуточных результатов обработки данных.	***Знать:*** - нормативные документы; - особенности анализа уязвимости автоматизированные систем; - основные виды уязвимости автоматизированных систем. ***Уметь:*** - анализировать уязвимости автоматизированных систем в соответствии с требованиями; - минимизировать количество потенциальных несоответствий. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками установки директив, определяющих работу автоматизированных систем; - навыками проведения анализа нор-

1	2	3	4	5
				мативных документов; - технологией ведения протокола работы системы с выводом промежуточных результатов обработки данных.
	ПК-7.3 Формулирует угрозы информационной безопасности исходя из выявленных характеристик автоматизированной системы	***Знать:*** - основы шифрования потоков данных; - основы использования средств защиты информации. ***Уметь:*** - выводить сообщения в случае возникновения нештатных ситуаций работы информационной системы; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками оценки защищенности информационной системы с учетом возможных угроз.	***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; - интегрировать средства защиты на программном уровне. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками установки программных средств защиты;	***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.
ПК-8/	ПК-8.1 Раз-	***Знать:*** перечень	***Знать:*** перечень	***Знать:*** методики

1	2	3	4	5
завершающий	рабатывает методическую, техническую, рекомендательную и отчётную документацию по анализу защищённости автоматизированной системы	угроз, на нейтрализацию которых направлены отдельные меры по защите информации ***Уметь:*** проводить отдельные мероприятия по обеспечению информационной безопасности в логически структурированные последовательности ***Владеть (****или* ***Иметь опыт деятельности):*** использования отдельных технологий обеспечения информационной безопасности в ТКС	угроз, на нейтрализацию которых направлена та или иная мера по защите информации ***Уметь:*** последовательно проводить отдельные мероприятия по обеспечению информационной безопасности в логически структурированные последовательности ***Владеть (****или* ***Иметь опыт деятельности):*** использования типовых технологий обеспечения информационной безопасности в ТКС	определения угроз, на нейтрализацию которых направлена та или иная мера по защите информации ***Уметь:*** объединять отдельные мероприятия по обеспечению информационной безопасности в логически структурированные последовательности ***Владеть (****или* ***Иметь опыт деятельности):*** использования разнообразных технологий обеспечения информационной безопасности в ТКС
	ПК-8.2 Осуществляет подбор программных средств тестирования защищённости автоматизированной системы в зависимости от предъявляемым к ней требованиям	***Знать:*** номенклатуру этапов работ по оценке уровня защищённости автоматизированных системы ***Уметь:*** проводить оценку отдельных характеристик защищённости автоматизированной системы ***Владеть (****или* ***Иметь опыт деятельности):*** навыками оценки отдельных характеристик автоматизированных систем	***Знать:*** последовательность работ по оценке уровня защищённости автоматизированных систем ***Уметь:*** проводить оценку уровня защищённости автоматизированной системы ***Владеть (****или* ***Иметь опыт деятельности):*** навыками контроля уровня защищённости автоматизированных систем	***Знать:*** методику и принципы оценки уровня защищённости автоматизированной системы ***Уметь:*** проводить оценку уровня защищённости сложной и нетиповой автоматизированной системы ***Владеть (****или* ***Иметь опыт деятельности):*** навыками контроля уровня защищённости сложной и нетиповой автоматизированной системы
	ПК-8.3 Использует средств инструментального анализа защищённо-	***Знать:*** отдельные уязвимости защищённости автоматизированных систем и угрозы автоматизированных систем	***Знать:*** уязвимости защищённости автоматизированных систем и угрозы автоматизированных систем ***Уметь:*** с помощью	***Знать:*** уязвимости защищённости автоматизированных систем и угрозы автоматизированных систем и методики их выявления

1	2	3	4	5
	сти программных и аппаратных платформ узлов автоматизированной системы	***Уметь:*** использовать инструментальные средства выявления уязвимостей защищённости автоматизированных систем ***Владеть (****или* ***Иметь опыт деятельности):*** навыками выявления типовых уязвимостей защищённости автоматизированных систем	инструментальных средств выявлять уязвимости защищённости автоматизированных систем ***Владеть (****или* ***Иметь опыт деятельности):*** навыками выявления уязвимостей защищённости автоматизированных систем	***Уметь:*** выявлять уязвимости защищённости автоматизированных систем комбинацией различных методов и средств ***Владеть (****или* ***Иметь опыт деятельности):*** навыками выявления уязвимостей защищённости автоматизированных систем, в том числе и не описанных в специализированных справочниках
	ПК-8.4 Проводит контроль защищённости и функционирования программно-аппаратных и технических средств автоматизированной системы	***Знать:*** отдельные уязвимости защищённости телекоммуникационных систем и сетей и угрозы автоматизированных систем ***Уметь:*** использовать инструментальные средства выявления уязвимостей защищённости телекоммуникационных систем и сетей ***Владеть (****или* ***Иметь опыт деятельности):*** навыками выявления типовых уязвимостей защищённости автоматизированных систем	***Знать:*** уязвимости защищённости телекоммуникационных систем и сетей и угрозы автоматизированных систем ***Уметь:*** с помощью инструментальных средств выявлять уязвимости защищённости телекоммуникационных систем и сетей ***Владеть (****или* ***Иметь опыт деятельности):*** навыками выявления уязвимостей защищённости автоматизированных систем	***Знать:*** уязвимости защищённости телекоммуникационных систем и сетей и угрозы автоматизированных систем и методики их выявления ***Уметь:*** выявлять уязвимости защищённости телекоммуникационных систем и сетей комбинацией различных методов и средств ***Владеть (****или* ***Иметь опыт деятельности):*** навыками выявления уязвимостей защищённости автоматизированных систем, в том числе и не описанных в специализированных справочниках
ПК-9/ завершающий	ПК-9.1 Формулирование правил работы персонала со	**Знать**: основные правила работы со средствами защиты информации. **Уметь**:	**Знать**: правила работы со средствами защиты информации. **Уметь**:	**Знать** в полной мере правила работы со средствами защиты информации. **Уметь**:

1	2	3	4	5
	средствами защиты информации	применять базовые правила работы с штатными средствами защиты информации. **Владеть навыками**: формулирования основных правил работы со средствами защиты информации.	применять правила работы со средствами защиты информации различных производителей. **Владеть навыками**: формулирования перечня правил обращения и работы со средствами защиты информации.	в полной мере применять правила работы со средствами защиты информации различных производителей. **Владеть навыками**: формулирования расширенного перечня правил обращения и работы со средствами защиты информации.
ПК-10/ завершающий	ПК-10.1 Соотносит инциденты информационной безопасности с характеристиками систем и средств защиты информации	Знать: типовые инциденты информационной безопасности АС. Уметь: классифицировать инциденты информационной безопасности АС. Владеть: навыками применения программных и аппаратных средств защиты информации в АС.	Знать: состав, документацию, характеристики и принцип работы оборудования АС. Уметь: применять средства защиты информации в АС, определять уязвимые узлы в системе информационной безопасности. Владеть: навыками обнаружения инцидентов и восстановления функционирования оборудования АС.	Знать: классификацию, состав, документацию, способы применения систем и средств защиты информации в АС. Уметь: осуществлять контроль функционирования систем и средств защиты АС, проводить анализ результатов выполняемых работ. Владеть: навыками контроля и анализа результатов выполняемых работ.
	ПК-10.4 Формулирует правила протоколирования результатов мониторинга безопасности автоматизированных систем	***Знать:*** задачи и функции систем и средств мониторинга и управления средствами обеспечения безопасности АС. Уметь: проводить анализ защищенности АС. Владеть: Навыками анализа	Знать: правила эксплуатации оборудования и программных средств управления средствами защиты АС. Уметь: разрабатывать правила протоколирования результатов мониторинга АС.	***З*** Знать: классификацию и способы применения средств и систем защиты АС. Уметь: настраивать оборудования и программных средств мониторинга и управления средствами защиты АС,

1	2	3	4	5
		защищенности АС	Владеть: навыками эксплуатации программных средств мониторинга и управления средствами зашиты АС.	средства и системы защиты АС. Владеть: навыками разработки правил протоколирования результатов мониторинга АС, настройки оборудования и программных средств мониторинга и управления средствами защиты АС, средств и систем защиты АС.

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
УК-1 завершающий	Дневник практики. Отчёт по практике с результатами измерений и отчётов
ПК-4 завершающий	Дневник практики. Отчет о практике. Доклад обучающегося на промежуточной аттестации (защита отчета о практике). Характеристика руководителя практики от организации управленческих качеств обучающегося.
ПК-5 завершающий	Дневник практики. Отчет о практике. Доклад обучающегося на промежуточной аттестации (защита отчета о практике). Характеристика руководителя практики от организации управленческих качеств обучающегося.
ПК-7 завершающий	Дневник практики. Отчет о практике. Типовое задание № 1 по практической подготовке, предусматри-

	вающее выполнение обучающимся вида(ов) работ, связанного(ых) с будущей профессиональной деятельностью (задание конкретизируется с учетом особенностей конкретной профильной организации в Дневнике практики, в п.1.4 задания студенту): *Подготовьте паспорт объекта информатизации для проведения аттестационных испытаний по защите информации.* Ответы на вопросы по содержанию практики на промежуточной аттестации.
ПК-8 завершающий	Отчет о практике. Типовое задание № 2 по практической подготовке, предусматривающее выполнение обучающимся вида(ов) работ, связанного(ых) с будущей профессиональной деятельностью (задание конкретизируется с учетом особенностей конкретной профильной организации в Дневнике практики, в п.1.4 задания студенту): *разработать модель угроз для объекта информатизации, на котором происходит эксплуатация автоматизированной ситсемы.* Разработанные модели угроз Ответы на вопросы по содержанию практики на промежуточной аттестации.
ПК-9 завершающий	Дневник практики. Типовое задание № 3 по практической подготовке, предусматривающее выполнение обучающимся вида(ов) работ, связанного(ых) с будущей профессиональной деятельностью (задание конкретизируется с учетом особенностей конкретной профильной организации в Дневнике практики, в п.1.4 задания студенту): *Разработайте рекомендации по повышению уровня безопасности предприятия, основываясь на результатах проведенного мониторинга (производственного контроля).* Графические материалы к отчету. Раздел отчета о практике – *Результаты проведенного мониторинга (и (или) производственного контроля) работоспособности ТКС.*
ПК-10 завершающий	Дневник практики. Разделы отчета о практике: *– Профили защиты используемых средств обеспечения информационной безопасности.* *– Защищённости ТКС.*

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
	измененных	замененных	аннулированных	новых			