МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФГБОУ ВО «Уральский государственный экономический университет»

Одобрена
на заседании кафедры

26.12. 2019 г.

протокол № 3

Зав. кафедрой Назаров Д.М.

Утверждена
Советом по учебно-методическим вопросам и качеству образования

15 января 2020 г.

протокол № 5

Председатель _____ Карх Д.А.
(подпись)

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

Вид практики	Производственная
Тип практики	Преддипломная практика
Направление подготовки	10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
Профиль	Информационно-аналитические системы финансового мониторинга
Форма обучения	очная
Год набора	2020

Разработана:
Профессор,д.э.н.
Назаров Д.М.

Екатеринбург
2020 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Программа практики является частью основной профессиональной образовательной программы высшего образования - программы бакалавриата, разработанной в соответствии с ФГОС ВО

ФГОС ВО	Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ (уровень бакалавриата) (приказ Минобрнауки России от

1. ЦЕЛЬ, ВИД, ТИП, СПОСОБ И ФОРМЫ ПРОВЕДЕНИЯ ПРАКТИКИ

Целью является формирования компетенций в соответствии с видами профессиональной деятельности, на которые ориентирована программа, для готовности к решениям профессиональных задач.

Вид практики: Производственная

Тип практики: Преддипломная практика

Способы проведения практики: стационарная

Формы проведения практики:

дискретно - по видам практик

Практика может быть проведена с использованием дистанционных образовательных технологий и электронного обучения.

2. МЕСТО ПРАКТИКИ В СТРУКТУРЕ ОПОП

Практика в полном объеме относится к вариативной части учебного плана.

3. ОБЪЕМ ПРАКТИКИ

Промежуточный контроль	Часов				З.е.
	Всего за семестр	Контактная работа .(по уч.зан.)		Самостоятельная работа в том числе подготовка контрольных и курсовых	
		Всего	Лекции		
Семестр 8					
Зачет с оценкой	216	2	2	214	6

4.ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ОПОП

В результате прохождения практики у обучающегося должны быть сформированы компетенции, установленные в соответствии ФГОС ВО.

Общекультурные компетенции (ОК)

Шифр и наименование компетенции	Индикаторы достижения компетенций

ОК-8 способностью к самоорганизации и самообразованию	ИД-1.ОК-8 Знает основные принципы самовоспитания и самообразования, профессионального и личностного развития, исходя из этапов карьерного роста и требований рынка труда. Умеет планировать свое рабочее время и время для саморазвития; формулировать цели личностного и профессионального развития и условия их достижения, исходя из тенденций развития области профессиональной деятельности, индивидуально-личностных особенностей. Владеет навыками планирования перспективных целей собственной деятельности с учетом условий, средств, личностных возможностей, этапов карьерного роста, временной перспективы развития деятельности и требований рынка труда; критической оценки эффективности использования времени и других ресурсов при решения поставленных задач, а также относительно полученного результата

Общепрофессиональные компетенции (ОПК)

Шифр и наименование компетенции	Индикаторы достижения компетенций
ОПК-5 способностью использовать нормативные правовые акты в профессиональной деятельности	ИД-1.ОПК-5 Знает основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации. Умеет применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности. Владеет навыками использования навыками использования нормативно-правовых актов в профессиональной деятельности.
ОПК-7 способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	ИД-1.ОПК-7 Знает уязвимости информационных ресурсов, возможные угрозы безопасности информации, информационные процессы объектов. Умеет определять информационные ресурсы, подлежащие защите информации, угрозы безопасности информации. Имеет навыки формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем; профессиональной терминологией в области обеспечения безопасности персональных данных; методами мониторинга и аудита, выявления угроз и управления информационной безопасностью.

Профессиональные компетенции (ПК)

Шифр и наименование компетенции	Индикаторы достижения компетенций
эксплуатационная	

ПК-2 способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	ИД-1.ПК-2 Знать: программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования. Уметь: выбирать и применять необходимые инструментальные средства для решения профессиональных задач. Владеть навыками работы в программные средства системного, прикладного и специального назначения, инструментальными средствами, языками и системами программирования.
экспериментально-исследовательская	
ПК-9 способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	ИД-1.ПК-9 Знать: основы информационной безопасности, отечественные и зарубежные стандарты оценки защищенности информационных систем, источники информации содержащей сведения по вопросам обеспечения информационной безопасности, нормативные документы, отечественные и зарубежные стандарты в данной сфере. Уметь: собирать и обобщать информацию, содержащуюся в различных формах отчетности и прочих источниках, подбирать, изучать и обобщать информацию по вопросам обеспечения информационной безопасности. Владеть навыками: сбора и обобщения информации, содержащейся в различных источниках, навыками сбора и обработки, анализа и интерпретации информации содержащей сведения по вопросам обеспечения информационной безопасности
ПК-10 способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	ИД-1.ПК-10 Знать: основы организации защиты государственной тайны и конфиденциальной информации; методы анализа информационной безопасности объектов и систем; стандарты в области информационной безопасности. Уметь: отечественные и зарубежные стандарты в области компьютерной безопасности и информационной безопасности объектов для проектирования, разработки и оценки защищенности компьютерных систем. Владеть: методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.
организационно-управленческая	
ПК-13 способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	ИД-1.ПК-13 Знать: политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации. Уметь: определять подлежащие защите информационные ресурсы автоматизированных систем; контролировать эффективность принятых мер по защите информации в автоматизированных системах. Владеть навыками: обоснования, выбора, реализации и контроля результатов управленческого решения, навыками выявления и устранения угроз информационной безопасности
ПК-14 способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности	ИД-1.ПК-14 Знать: основы управленческих подходов организации малой группы. Уметь: организовать деятельность малой группы. Иметь навыки (трудовые действия) реализации конкретного проекта в рамках малой группы.

ПК-15 способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ИД-1.ПК-15 Знать: основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области. Уметь: пользоваться нормативными документами по защите информации; обеспечивать сохранность и неизменность обрабатываемой информации. Владеть навыками: защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

Шифр и наименование компетенции	Индикаторы достижения компетенций
профессионально-специализированная	
ПСК-1 способность решать задачи первичного финансового мониторинга в рамках функционирования служб внутреннего контроля субъектов финансового мониторинга	ИД-1.ПСК-1 Знать: сущность первичного финансового мониторинга; особенности функционирования служб внутреннего контроля; основные составляющие финансовой и налоговой отчетности; положения нормативно-правовых документов в сфере противодействия легализации (отмыванию) доходов, полученных преступным путем. Уметь: анализировать финансовые операции (сделки) клиентов организации в деталях выявления их связи с ОД/ФТ, анализировать материалы финансовых расследований, схем отмывания преступных доходов в целях ПОД/ФТ; самостоятельно использовать теоретические знания методов первичного финансового мониторинга; применять на практике навыки по реализации системы внутреннего контроля и идентификации клиентов; выявлять операции, подлежащие обязательному контролю, а также операции, попадающие подкритерии и признаки необычных сделок. Владеть навыками: решения первичного финансового мониторинга; реализации политики финансового мониторинга в организациях, осуществляющих операции с денежными средствами или иным имуществом, системы внутреннего контроля в целях ПОД/ФТ; процедурами идентификации сомнительных сделок клиентов в процессе банковского обслуживания
ПСК-3 способность участвовать в разработке информационно-аналитических систем финансового мониторинга	ИД-1.ПСК-3 Знать: особенности разработки информационно-аналитических систем финансового мониторинга; современные технологии проектирования информационно-аналитических систем; основы функционирования информационно-аналитических систем финансового мониторинга. Уметь: ориентироваться в современных технологиях проектирования и эксплуатации информационных и аналитических систем; использовать современные технологии автоматизации проектной деятельности; применять на практике приемы и методы разработки информационно- аналитических систем. Владеть навыками: современными технологиями проектирования информационно-аналитических систем; методами построения, проектирования и эксплуатации информационно-аналитических систем финансового мониторинга; основными методами ресурсного планирования при разработке информационно-аналитических систем

ПСК-4 способность реализовывать комплекс мероприятий по защите информации в автоматизированных системах финансовых и экономических структур	ИД-1.ПСК-4 Знать: перечень и содержание мероприятий по защите информации в автоматизированных системах; особенности программно-аппаратных средств защиты информации; особенности защиты информации в автоматизированных системах финансовых и экономических структур; основные подходы к выбору мероприятий по защите информации в автоматизированных системах финансовых и экономических структур с помощью современных методов и средств Уметь: эффективно использовать современные программно-аппаратные средства защиты информации. обоснованно выбирать наиболее подходящие методы и средства защиты информации в автоматизированных системах финансовых и экономических структур; формулировать и реализовывать политику безопасности в системах финансовых и экономических структур. Владеть навыками: использования новых образцов программно-технических средств и информационных технологий, направленных на защиту информации в автоматизированных системах финансовых и экономических структур; методами и средствами выявления угроз безопасности автоматизированных систем; приемами и методами проведения мероприятий по защите информации в

Профессиональные компетенции (ПК)

Шифр и наименование компетенции	Индикаторы достижения компетенций
эксплуатационная	
ПК-1 способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	ИД-1.ПК-1 Знать: типовые средства и методы защиты информации в локальных и глобальных вычислительных сетях; базовую конфигурацию системы защиты информации автоматизированной системы, особенности применения программных и программно-аппаратных средств защиты информации в автоматизированных системах; типовые средства, методы и протоколы идентификации, аутентификации и авторизации; технические средства контроля эффективности мер защиты информации; Уметь: настраивать политики безопасности наиболее распространенных операционных систем, вычислительных сетей, противодействовать нарушениям сетевой безопасности, устанавливать, настраивать и обслуживать технические и программно-аппаратные средства защиты информации. Владеть навыками по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации

ПК-3 способностью администрировать подсистемы информационной безопасности объекта защиты	ИД-1.ПК-3 Знать: подсистемы информационной безопасности в сетях и системах передачи; перспективные современные методы и способы эксплуатации и администрирования телекоммуникационных систем; методику проведения настройки, наладки телекоммуникационного оборудования, используемого в сетях доступа; механизм функционирования основных подсистем администрирования объектов защиты на уровне администратора безопасности. Уметь: администрировать подсистемы информационной безопасности в телекоммуникационных сетях и системах; производить настройки, наладки телекоммуникационного оборудования, используемого в сетях доступа; администрировать современные программные средства на объектах защиты на уровне администратора безопасности. Владеть навыками: администрирования подсистемы информационной безопасности в сетях и системах передачи информации; эксплуатации и администрирования телекоммуникационных систем; навыками настройки, наладки телекоммуникационного оборудования, используемого в сетях доступа; навыками работы администратора программных средств
ПК-4 способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	ИД-1.ПК-4 Знать: современные подходы к управлению ИБ и направлениях их развития; основные стандарты, регламентирующие управление ИБ; принципы построения СУИБ; принципы разработки процессов управления ИБ; взаимосвязи отдельных процессов управления ИБ в рамках общей СУИБ; подходы к интеграции СУИБ в общую систему управления предприятием. Уметь: анализировать текущее состояние ИБ на предприятии с целью разработки требований к разрабатываемым процессам управления ИБ; определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ; применять процессный подход к управлению ИБ в различных сферах деятельности; используя современные методы и средства разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность; практически решать задачи формализации разрабатываемых процессов управления ИБ; разрабатывать и внедрять СУИБ и оценивать ее эффективность. Владеть навыками: навыками управления информационной безопасностью простых объектов; терминологией и процессным подходом построения систем управления ИБ; навыками анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ; навыками построения как отдельных процессов

ПК-5 способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	ИД-1.ПК-5 Знать: организацию аттестации объектов по требованиям безопасности информации; способностью организовать проведение и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов; виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия; инструментальные средства и системы программирования для решения профессиональных задач. Уметь: формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности; проводить предварительный технико-экономический анализ и обоснование проектных решений по обеспечению информационной безопасности; оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности. Владеть навыками: способами организации и проведения (сопровождения) аттестации объекта на соответствие требованиям государственных или корпоративных нормативных документов; профессиональной терминологией; навыками использования технических средств в профессиональной деятельности
ПК-6 способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	ИД-1.ПК-6 Знать: критерии оценки эффективности программных, программно-аппаратных и технических средств защиты информации. Уметь: проводить проверку работоспособности программных, программно-аппаратных и технических средств защиты информации; проводить оценку эффективности программных, программно-аппаратных и технических средств защиты информации. Владеть способностью: принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации.
проектно-технологическая	
ПК-7 способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	ИД-1.ПК-7 Знать: методы проектирования автоматизированных систем; основные принципы проектного управления. Уметь: проектировать и сопровождать типовые специализированные автоматизированные информационные системы, локальные сети; осуществлять подготовку технико-экономических обоснований соответствующих проектных решений. Владеть навыками: навыками определения затрат компании на информационную безопасность и проведения зависимости между затратами и уровнем защищенности.
ПК-8 способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	ИД-1.ПК-8 Знать: требования основных действующих государственных стандартов (ГОСТ) регламентирующие построение, проектирование и эксплуатацию информационных и аналитических систем. Уметь: осуществлять подготовку технических заданий на построение и проектирование информационных и аналитических систем; осуществлять подготовку организационно-распорядительной документации (инструкции, приказы, распоряжения) регламентирующей эксплуатацию информационных систем. Владеть навыками: оформления рабочей технической документации.

экспериментально-исследовательская	
ПК-11 способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	ИД-1.ПК-11 Знать: основные принципы экспериментальных исследований, соотношение теоретического и экспериментального знания. Уметь: разбираться в лабораторном оборудовании по профилю своей деятельности и работать с оборудованием для проведения экспериментов, применять методики, обрабатывать результаты, проводить оценку погрешности. Владеть навыками: выполнения расчетов, обработки результатов экспериментов, оценки погрешностей и достоверности результатов
ПК-12 способностью принимать участие в проведении экспериментальных исследований системы защиты информации	ИД-1.ПК-12 Знать: методику проведения экспериментальных исследований системы защиты информационной безопасности. Уметь: проводить экспериментально-исследовательские работы системы защиты информации. Владеть навыками: навыками проведения экспериментально-исследовательских работ системы защиты информации.

Шифр и наименование компетенции	Индикаторы достижения компетенций
профессионально-специализированная	
ПСК-2 способность учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах финансовых и экономических структур, для информационно-аналитического обеспечения финансового мониторинга	ИД-1.ПСК-2 Знать: особенности информационных технологий, применяемых в автоматизированных системах финансовых и экономических структур; сущность информационно-аналитической работы; особенности функционирования информационно-аналитической службы. Уметь: применять современные информационные технологии в автоматизированных системах финансовых и экономических структур; использовать математический аппарат анализа данных в информационно-аналитической работе. Владеть: основными приемами информационно-аналитической работы; навыками работы с современными информационно-аналитическими технологиями, используемыми для информационно-аналитического обеспечения финансового мониторинга; методами сбора, обработки аналитической информации для обеспечения финансового мониторинга; методами ресурсного планирования информационно-аналитической работы

5. ТЕМАТИЧЕСКИЙ ПЛАН

Тема	Часов						
	Наименование темы	Всего часов	Контактная работа .(по уч.зан.)			Самост. работа	Контроль самостоятельной работы
			Лекции	Лабораторные	Практические занятия		
Семестр 8		36					
Этап 1.	Знакомство с основными бизнес-процессами организации	36	2			34	
Семестр 8		80					
Этап 2.	Изучение проблем, уязвимостей в сетях предприятия	80				80	
Семестр 8		100					

Этап 3.	Анализ выбранного этапа осуществления информационной безопасности.	100				100	

6. ФОРМЫ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ШКАЛЫ ОЦЕНИВАНИЯ

Раздел/ Этап	Вид оценочного средства	Описание оценочного средства	Критерии оценивания
Текущий контроль			
Этап 1	Отчет и приложение к отчету	Аналитическая записка	< 50 - неуд 51<...<70 - удовл 71<...<84 - хор >85 - отл
Этап 2	Отчет и приложение к отчету	Приложение 2 к отчету	< 50 - неуд 51<...<70 - удовл 71<...<84 - хор >85 - отл
Этап 3	Отчет и приложение к отчету	Приложение 3 к отчету	< 50 - неуд 51<...<70 - удовл 71<...<84 - хор >85 - отл
Промежуточный контроль			
8 семестр (ЗаО)	Отчет	Кейс	< 50 - неуд 51<...<70 - удовл 71<...<84 - хор >85 - отл

ОПИСАНИЕ ШКАЛ ОЦЕНИВАНИЯ

Текущий контроль. Используется 100-балльная система оценивания. В течении практики руководители практики от профильной организации и университета осуществляют контроль в соответствии с совместным планом и индивидуальным планом обучающегося. В отчете обучающегося ставится процент выполнения и отметка «выполнено/не выполнено»

Промежуточная аттестация. Используется рейтинговая система оценивания. Оценка работы обучающегося по окончанию практики осуществляется руководителем практики от университета в соответствии с разработанной им системой оценки достижений студента в процессе практики.

Порядок перевода рейтинга, предусмотренных системой оценивания:

Высокий уровень – 100% - 70% - отлично, хорошо, зачтено.

Средний уровень – 69% - 50% - удовлетворительно, зачтено.

Показатель оценки	По 5-балльной системе	Характеристика показателя
100% - 85%	отлично	обладают теоретическими знаниями в полном объеме, понимают, самостоятельно умеют применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов на высоком уровне
84% - 70%	хорошо	обладают теоретическими знаниями в полном объеме, понимают, самостоятельно умеют применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов. Могут быть допущены недочеты, исправленные студентом самостоятельно в процессе работы (ответа и т.д.)
69% - 50%	удовлетворительно	обладают общими теоретическими знаниями, умеют применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов на среднем уровне. Допускаются ошибки, которые студент затрудняется исправить самостоятельно.
49 % и менее	неудовлетворительно	обладают не полным объемом общих теоретическими знаниями, не умеют самостоятельно применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов. Не сформированы умения и навыки для решения
100% - 50%	зачтено	характеристика показателя соответствует «отлично», «хорошо», «удовлетворительно»
49 % и менее	не зачтено	характеристика показателя соответствует «неудовлетворительно»

7. СОДЕРЖАНИЕ ПРАКТИКИ

7.1. Содержание лекций

Этап 1. Знакомство с основными бизнес-процессами организации Проведение инструктажа на месте прохождения практики. Знакомство с руководителем, определение видов деятельности студента на время прохождения практики.

7.3. Содержание самостоятельной работы

Этап 1. Знакомство с основными бизнес-процессами организации Совершенствование навыков использования современных средств и инструментов информационной безопасности, работа с нормативными документами организации, знакомство с основными бизнес- процессами.
Этап 2. Изучение проблем, уязвимостей в сетях предприятия Участие в осуществлении бизнес-процессов конкретной организации в соответствии с планом практики и поставленной индивидуальной задачей. Выполнение задания по поручению и под наблюдением работника отдела информационной безопасности (руководителя или специалиста ИТ-отдела, инженера по информационной безопасности). Участие в работе отдела в качестве наблюдателя. Изучение проблем, уязвимостей в сетях предприятия
Этап 3. Анализ выбранного этапа осуществления информационной безопасности. Осуществление сбора, обработки, анализа и систематизации информации по этапам и процессам осуществления информационной безопасности. Анализ выбранного этапа осуществления информационной безопасности. Анализ документации и электронных ресурсов организации

7.3.1.Совместный рабочий график проведения практики

Приложение 1

7.3.2. Индивидуальное задание
Приложение 2

7.3.3. . Фонд оценочных средств для проведения промежуточной аттестации обучающихся по практике
Приложение 3

7.4. Отчет по практике
Отчет по практике размещается в портфолио
приложение 4

8. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ПРАКТИКИ ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Практика для обучающихся с ограниченными возможностями здоровья и инвалидов проводится с учетом особенностей их психофизического развития, индивидуальных возможностей и состояния здоровья.

По заявлению студента

В целях доступности прохождения практики профильная организация и УрГЭУ обеспечивают следующие условия:

- особый порядок прохождения практики, с учетом состояния их здоровья в формах, адаптированных к ограничениям их здоровья;
- применение дистанционные образовательные технологии, которые предусматривают возможности приема-передачи информации в доступных для них формах.
- доступ (удаленный доступ), к современным профессиональным базам данных и информационным справочным системам, состав которых определен рабочей программой практики.

9. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ПРОХОЖДЕНИЯ ПРАКТИКИ

Сайт библиотеки УрГЭУ

http://lib.usue.ru/

Основная литература:

1. Буценко Е. В.. Экономика защиты информации [Электронный ресурс]:учебное пособие. - Екатеринбург: [Издательство УрГЭУ], 2018. - 108 с. – Режим доступа: http://lib.usue.ru/resource/limit/ump/18/p491459.pdf

2. Партыка Т. Л., Попов И. И.. Информационная безопасность [Электронный ресурс]:учебное пособие для студентов учреждений среднего профессионального образования, обучающихся по специальностям информатики и вычислительной техники. - Москва: ФОРУМ: ИНФРА-М, 2018. - 432 с. – Режим доступа: http://znanium.com/go.php?id=915902

3. Маркова В. Д.. Цифровая экономика [Электронный ресурс]:учебник для студентов вузов, обучающихся по направлениям подготовки 38.03.02 "Менеджмент", 38.03.01 "Экономика" (квалификация (степень) "бакалавр"). - Москва: ИНФРА-М, 2018. - 186 с. – Режим доступа: http://znanium.com/go.php?id=959818

4. Бабаш А. В., Баранова Е. К., Ларин Д. А.. Информационная безопасность. История специальных методов криптографической деятельности [Электронный ресурс]:учебное пособие. - Москва: РИОР: ИНФРА-М, 2019. - 236 с. – Режим доступа: http://znanium.com/go.php?id=987215

5. Партыка Т. Л., Попов И. И.. Информационная безопасность [Электронный ресурс]:учебное пособие для студентов учреждений среднего профессионального образования, обучающихся по специальностям информатики и вычислительной техники. - Москва: Форум: ИНФРА-М, 2019. - 432 с. – Режим доступа: http://znanium.com/go.php?id=987326

6. Бабаш А. В., Баранова Е. К.. Актуальные вопросы защиты информации [Электронный ресурс]:монография. - Москва: РИОР: ИНФРА-М, 2018. - 111 с. – Режим доступа: http://znanium.com/go.php?id=979073

7. Шаньгин В. Ф.. Комплексная защита информации в корпоративных системах [Электронный ресурс]:учебное пособие для студентов вузов, обучающихся по направлению 09.03.01 "Информатика и вычислительная техника". - Москва: ФОРУМ: ИНФРА-М, 2019. - 592 с. – Режим доступа: http://znanium.com/go.php?id=996789

8. Баранова Е. К., Бабаш А. В.. Информационная безопасность и защита информации [Электронный ресурс]:учебное пособие для студентов, обучающихся по направлению "Прикладная информатика". - Москва: РИОР: ИНФРА-М, 2019. - 336 с. – Режим доступа: http://znanium.com/go.php?id=1009606

9. Шаньгин В. Ф.. Информационная безопасность компьютерных систем и сетей [Электронный ресурс]:учебное пособие для студентов учреждений среднего профессионального образования, обучающихся по группе специальностей 09.00.00 «Информатика и вычислительная техника». - Москва: ФОРУМ: ИНФРА-М, 2019. - 416 с. – Режим доступа: http://znanium.com/go.php?id=1009605

10. Баранова Е.К., Бабаш А.В.. Основы информационной безопасности [Электронный ресурс]:учебник. - Москва: РИОР: ИНФРА-М, 2019. - 202 с. – Режим доступа: http://znanium.com/go.php?id=1014830znanium.com

11. Шевчук П. С., Соколов С. В., Крамаров С.О., Тищенко Е.Н., Митясова О. Ю., Крамаров С.О.. Криптографическая защита информации [Электронный ресурс]:учебное пособие. - Москва: РИОР: ИНФРА-М, 2019. - 324 с. – Режим доступа: http://znanium.com/go.php?id=1018903znanium.com

12. Мартишин С. А., Симонов В. Л., Храпченко М. В.. Основы теории надежности информационных систем [Электронный ресурс]:учебного пособия для студентов высших учебных заведений, обучающихся по направлению 09.03.02 «Информационные системы и технологии». - Москва: ФОРУМ: ИНФРА-М, 2019. - 255 с. – Режим доступа: http://znanium.com/go.php?id=1019400znanium.com

13. Романьков В. А.. Введение в криптографию. Курс лекций [Электронный ресурс]:учебное пособие для студентов вузов, обучающихся по направлениям подготовки 01.03.01 "Математика", 02.03.01 "Математика и компьютерные технологии", 01.03.02 "Прикладная математика и информатика" (квалификация (степень) "бакалавр"). - Москва: ФОРУМ: ИНФРА-М, 2019. - 240 с. – Режим доступа: http://znanium.com/go.php?id=1018899znanium.com

14. Щеглов А. Ю., Щеглов К. А.. Защита информации: основы теории [Электронный ресурс]:учебник для бакалавриата и магистратуры: для студентов вузов, обучающихся по инженерно -техническим направлениям. - Москва: Юрайт, 2019. - 309 с. – Режим доступа: https://www.biblio- online.ru/bcode/433715

15. Сычев Ю. Н.. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов [Электронный ресурс]:учебное пособия для студентов вузов, обучающихся по укрупненной группе специальностей и направлений 10.03.00 «Информационная безопасность». - Москва: ИНФРА-М, 2019. - 223 с. – Режим доступа: http://znanium.com/go.php?id=979415znanium.com

16. Гришина Н. В.. Основы информационной безопасности предприятия [Электронный ресурс]:учебное пособие для студентов вузов, обучающихся по направлению подготовки 10.03.01 "Информационная безопасность" (квалификация (степень) "бакалавр"). - Москва: ИНФРА-М, 2019. - 216 с. – Режим доступа: http://znanium.com/go.php?id=1017663znanium.com

17. Овчинский В. С.. Криминология цифрового мира [Электронный ресурс]:учебник для магистратуры. - Москва: Норма: ИНФРА-М, 2020. - 352 с. – Режим доступа: https://new.znanium.com/catalog/product/1059377

18. Баранова Е.К., Бабаш А.В.. Актуальные вопросы защиты информации [Электронный ресурс]:Монография. - Москва: Издательский Центр РИО, 2020. - 111 с. – Режим доступа: http://new.znanium.com/go.php?id=1052207

19. Мартишин С.А., Симонов В.Л.. Основы теории надежности информационных систем [Электронный ресурс]:Учебное пособие. - Москва: Издательский Дом "ФОРУМ", 2020. - 255 с. – Режим доступа: http://new.znanium.com/go.php?id=1062374

20. Клименко И.С.. Информационная безопасность и защита информации: модели и методы управления [Электронный ресурс]:Монография. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2020. - 180 с. – Режим доступа: http://new.znanium.com/go.php?id=1018665

21. Степанов О. А.. Противодействие кибертерроризму в цифровую эпоху [Электронный ресурс]:Монография. - Москва: Издательство Юрайт, 2020. - 103 с. – Режим доступа: https://www.biblio-online.ru/bcode/448300

22. Шульц В. Л., Юрченко А. В., Рудченко А. Д.. Безопасность предпринимательской деятельности [Электронный ресурс]:Учебник для вузов. - Москва: Юрайт, 2020. - 585 с – Режим доступа: https://urait.ru/bcode/447405

Дополнительная литература:

1. Домашев А. В., Попов В. О., Правиков Д. И., Прокофьев И. В., Щербаков А. Ю.. Программирование алгоритмов защиты информации:учебное пособие. - Москва: Нолидж, 2000. - 279 с.

2. Степанов Е. А., Корнеев И. К.. Информационная безопасность и защита информации:учебное пособие для вузов по специальности "Документоведение и документац. обеспечение упр.". - Москва: ИНФРА-М, 2001. - 304 с.

3. Завгородний В. И.. Комплексная защита информации в компьютерных системах:учебное пособие для студентов вузов. - Москва: Логос, 2001. - 263 с.

4. Зегжда Д. П., Ивашко А. М.. Основы безопасности информационных систем:учебник для студентов вузов, обучающихся по специальности "Компьютерная безопасность" и "Комплексное обеспечение информац..... - Москва: Горячая линия-Телеком, 2000. - 452 с.

5. Одинцов А. А.. Экономическая и информационная безопасность:справочник: учебное пособие для студентов вузов, обучающихся по специальности "Национальная экономика" и другим экономическим специальностям. - Москва: Экзамен, 2005. - 575 с.

6. Садердинов А. А., Трайнев В. А., Федулов А. А.. Информационная безопасность предприятия:учебное пособие. - Москва: Дашков и К°, 2004. - 335 с.

7. Гончаренко Л. П., Куценко Е. С.. Управление безопасностью:учебное пособие. - Москва: КНОРУС, 2005. - 272 с.

8. Садердинов А. А., Трайнев В. А., Федулов А. А.. Информационная безопасность предприятия:учебное пособие. - Москва: Дашков и К°, 2007. - 335 с.

9. Цирлов В. Л.. Основы информационной безопасности:краткий курс. - Ростов-на-Дону: Феникс, 2008. - 254 с.

10. Минаев В. А., Фисун А. П., Скрыль С. В., Дворянкин С. В., Никитин М. М., Хохлов Н. С., Минаев В. А., Фисун А. П., Скрыль С. В., Дворянкин С. В., Никитин М. М., Хохлов Н. С.. Правовое обеспечение информационной безопасности:учебник для курсантов и слушателей образовательных учреждений высшего профессионального образования МВД России по специальности 090106 - "Информационная безопасность телекоммуникационных систем". - Москва: Маросейка, 2008. - 368 с.

10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ЛИЦЕНЗИОННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ, ОНЛАЙН КУРСОВ, ИСПОЛЬЗУЕМЫХ ПРИ ПРОХОЖДЕНИИ ПРАКТИКИ

Перечень лицензионного программного обеспечения:

Astra Linux Common Edition. Договр № 1 от 13 июня 2018, акт от 17 декабря 2018. Срок действия лицензии - без органичения срока.

МойОфис стандартный. Соглашение № СК-281 от 7 июня 2017. Дата заключения - 07.06.2017. Срок действия лицензии - без органичения срока.

Microsoft Windows 10 .Договор № 52/223-ПО/2020 от 13.04.2020, Акт № Tr000523459 от 14.10.2020. Срок действия лицензии 30.09.2023.

Microsoft Office 2016.Договор № 52/223-ПО/2020 от 13.04.2020, Акт № Tr000523459 от 14.10.2020 Срок действия лицензии 30.09.2023.

Язык программирования R.Лицензия GNU GPL 2.Срок действия лицензии - без органичения срока.

R Studio (среда для языка программирования R).Лицензия GNU Affero General Public License v3.Срок действия лицензии - без органичения срока.

IBLite XE7. Эл. лицензия, Информационное письмо.

Microsoft SQL Server Express. Лицензия для образовательных учреждений. Срок действия лицензии - без органичения срока.

СЗИ от НСД "Страж NT" версия 4.0. Договор № 73700092 от 04.08.2017,Товарная накладная № 73700092 от 11.10.2017.

Secret Net 7. Клиент (автономный режим работы). Договор № 73700092 от 04.08.2017, Товарная накладная № 73700092 от 11.10.2017.

Oracle VM VirtualBox. СПО. Срок действия лицензии - без органичения срока.

Эмулятор GNS 3.Лицензия GNU GPL. Срок действия лицензии - без органичения срока.

Nmap security scanner.Лицензия GPL v2. Срок действия лицензии - без органичения срока.

Система контроля версий Git. Лицензия GNU GPL v2 and GNU LGPL v2.1. Срок действия лицензии - без органичения срока.

Notepad++. Лицензия GNU General Public License. Срок действия лицензии - без органичения срока.

HxD Hex Editor. Лицензия freeeware. Срок действия лицензии - без органичения срока.

Перечень информационных справочных систем, ресурсов информационно-телекоммуникационной сети «Интернет»:

Справочно-правовая система Гарант. Договор № 58419 от 22 декабря 2015. Срок действия лицензии -без ограничения срока

-Справочно-правовая система Консультант +. Договор № 194-У-2019 от 09.01.2020. Срок действия лицензии до 31.12.2020

11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ПРОХОЖДЕНИЯ ПРАКТИКИ

Реализация практики осуществляется с использованием материально-технической базы УрГЭУ и профильной организации (при необходимости).

Рабочие места и помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду УрГЭУ и профильной организации (при наличии).

Все помещения укомплектованы специализированной мебелью и оснащены мультимедийным оборудованием спецоборудованием (информационно-телекоммуникационным, иным компьютерным), доступом к информационно-поисковым, справочно-правовым системам, электронным библиотечным системам, базам данных действующего законодательства, иным информационным ресурсам служащими для представления учебной информации большой аудитории.