

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Силин Яков Петрович
Должность: Ректор
Дата подписания: 03.02.2022 12:30:01
Уникальный программный идентификатор:
24f866be2aca164840368cb3c5099531b605f

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	Учебная
Тип практики	Технологическая практика
Направление подготовки	10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
Профиль	Информационно-аналитические системы финансового мониторинга
Форма обучения	очная
Год набора	2020
Разработана:	
Доцент, к.ф.м.н.	
Ефимов Константин Сергеевич	

Екатеринбург
2020 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	3
1. ЦЕЛЬ, ВИД, ТИП, СПОСОБ (ПРИ НАЛИЧИИ) И ФОРМЫ ПРОВЕДЕНИЯ ПРАКТИКИ	3
2. МЕСТО ПРАКТИКИ В СТРУКТУРЕ ОПОП	3
3. ОБЪЕМ ПРАКТИКИ	3
4. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ОПОП	3
5. ТЕМАТИЧЕСКИЙ ПЛАН	6
6. ФОРМЫ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ШКАЛЫ ОЦЕНИВАНИЯ	6
7. СОДЕРЖАНИЕ ПРАКТИКИ	8
8. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ПРАКТИКИ ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ	9
9. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ПРОХОЖДЕНИЯ ПРАКТИКИ	10
10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ЛИЦЕНЗИОННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ, ОНЛАЙН КУРСОВ, ИСПОЛЬЗУЕМЫХ ПРИ ПРОХОЖДЕНИИ ПРАКТИКИ	10
11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ПРОХОЖДЕНИЯ ПРАКТИКИ	11

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: Учебная

Тип практики: Технологическая 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 5					
Зачет с оценкой	108	2	2	106	3

4. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ОПОП

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

Общепрофессиональные компетенции (ОПК)

Шифр и наименование компетенции	Индикаторы достижения компетенций
---------------------------------	-----------------------------------

<p>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</p>	<p>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.</p>
--	--

Профессиональные компетенции (ПК)

Шифр и наименование компетенции	Индикаторы достижения компетенций
эксплуатационная	
<p>ПК-1 способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации</p>	<p>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</p>
<p>ПК-3 способностью администрировать подсистемы информационной безопасности объекта защиты</p>	<p>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;</p>

<p>ПК-4 способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты</p>	<p>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.</p> <p>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.</p> <p>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</p>
<p>ПК-5 способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации</p>	<p>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.</p> <p>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.</p> <p>Владеть навыками: способами организации и проведения (сопровождения) аттестации объекта на соответствие требованиям государственных или корпоративных нормативных документов; профессиональной терминологией; навыками использования</p>
<p>ПК-6 способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации</p>	<p>ИД-1.ПК-6 Знать: критерии оценки эффективности программных, программно-аппаратных и технических средств защиты информации.</p> <p>Уметь: проводить проверку работоспособности программных, программно-аппаратных и технических средств защиты информации; проводить оценку эффективности программных, программно-аппаратных и технических средств защиты информации.</p> <p>Владеть способностью: принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации.</p>

5. ТЕМАТИЧЕСКИЙ ПЛАН

Тема	Часов						
	Наименование темы	Всего часов	Контактная работа (по уч.зан.)			Самост. работа	Контроль самостоятельной работы
			Лекции	Лабораторные	Практические занятия		
Семестр 5		32					
Этап 1.	Знакомство с основными бизнес-процессами	32	2			30	
Семестр 5		50					
Этап 2.	Изучение проблем, уязвимостей в сетях предприятия	50				50	
Семестр 5		26					
Этап 3.	Анализ выбранного этапа осуществления информационной	26				26	

6. ФОРМЫ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ШКАЛЫ ОЦЕНИВАНИЯ

Раздел/Тема	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			
5 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
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
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. Башлы П. Н., Бабаш А. В., Баранова Е. К.. Информационная безопасность и защита информации:учебник. - Москва: РИОР, 2013. - 222 с.
2. Партыка Т. Л., Попов И. И.. Информационная безопасность:учебное пособие для студентов учреждений среднего профессионального образования, обучающихся по специальностям информатики и вычислительной техники. - Москва: ФОРУМ: ИНФРА-М, 2018. - 432 с.
3. Трофимов В. В., Ильина О. П., Барабанова М. И., Кияев В. И., Трофимова Е. В.. Информационные технологии в экономике и управлении в 2 ч. Часть 1 [Электронный ресурс]:Учебник. - Москва: Издательство Юрайт, 2019. - 269 – Режим доступа: <https://www.biblio-online.ru/bcode/442379>

Дополнительная литература:

1. Шаньгин В. Ф.. Информационная безопасность компьютерных систем и сетей:учебное пособие для студентов учреждений среднего профессионального образования, обучающихся по группе специальностей 09.00.00 "Информатика и вычислительная техника". - Москва: ФОРУМ: ИНФРА-М, 2017. - 416 с.
2. Ковалев Д. В., Богданова Е. А.. Информационная безопасность:учебное пособие. - Ростов-на-Дону: Издательство Южного федерального университета (ЮФУ), 2016. - 74 с.
3. Минина Т. Б., Возмилов И. Д.. Организация научно-исследовательской работы студентов [Электронный ресурс]:учебное пособие. - Екатеринбург: [Издательство УрГЭУ], 2018. - 93 с. – Режим доступа: <http://lib.usue.ru/resource/limit/ump/18/p490910.pdf>

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

Перечень лицензионного программного обеспечения:

- Microsoft Windows 10 .Договор № 52/223-ПО/2020 от 13.04.2020, Акт № Tr000523459 от 14.10.2020. Срок действия лицензии 30.09.2023.
- Astra Linux Common Edition. Договр № 1 от 13 июня 2018, акт от 17 декабря 2018. Срок действия лицензии - без ограничения срока.
- Microsoft Office 2016.Договор № 52/223-ПО/2020 от 13.04.2020, Акт № Tr000523459 от 14.10.2020 Срок действия лицензии 30.09.2023.
- МойОфис стандартный. Соглашение № СК-281 от 7 июня 2017. Дата заключения - 07.06.2017. Срок действия лицензии - без ограничения срока.
- Libre Office. Лицензия GNU LGPL. Срок действия лицензии - без ограничения срока.
- Язык программирования R.Лицензия GNU GPL 2.Срок действия лицензии - без ограничения срока.
- R Studio (среда для языка программирования R).Лицензия GNU Affero General Public License v3.Срок действия лицензии - без ограничения срока.
- Язык программирования Python.Python Software Foundation License (PSFL). Срок действия лицензии - без ограничения срока.
- Secret Net 7. Клиент (автономный режим работы). Договор № 73700092 от 04.08.2017, Товарная накладная № 73700092 от 11.10.2017.
- Язык программирования Java.

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

1. Сайт Министерства информационных технологий и связи

: <http://www.minsvyaz.ru/>

2. Сайт совета безопасности РФ.

<http://www.scrf.gov.ru/documents/6/>

3. Вирусная библиотека

www.viruslist.com

4. Онлайн сканер

<http://www.kaspersky.ru/virusscanner>

9. Консультант плюс – онлайн версия

<http://www.consultant.ru/popular>

10. Интернет-университет информационных технологий «ИНТУИТ»

<http://www.intuit.ru>

ЭБС издательства «ЛАНЬ»

<http://e.lanbook.com/>

ЭБС Znanium.com

<http://znanium.com/>

Сетевое издание «Информационный ресурс СПАРК»

<http://www.spark-interfax.ru/>

Университетская информационная система РОССИЯ

<https://uisrussia.msu.ru/>

Архив научных журналов NEICON

<http://archive.neicon.ru>

Научная электронная библиотека КиберЛенинка

<http://cyberleninka.ru>

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.