МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФГБОУ ВО «Уральский государственный экономический университет»

Одобрена
на заседании кафедры

05.12.2022 г.

протокол № 4

Зав. кафедрой Назаров Д.М.

Утверждена
Советом по учебно-методическим
вопросам и качеству образования

14 декабря 2022 г.

протокол № 4

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	2023

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

Екатеринбург
2022 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 - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность (приказ Минобрнауки России от 17.11.2020 г. № 1427)

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	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.

Профессиональные компетенции (ПК)

Шифр и наименование компетенции	Индикаторы достижения компетенций
эксплуатационный	

ПК-1 Администрирование подсистем защиты информации в операционных системах	ИД-1.ПК-1 Знать: Архитектура и принципы построения операционных систем Программные интерфейсы операционных систем Виды политик управления доступом и информационными потоками применительно к операционным системам Архитектура подсистем защиты информации в операционных системах Принципы функционирования средств защиты информации в операционных системах, в том числе использующих криптографические алгоритмы Состав типовых конфигураций программно-аппаратных средств защиты информации Требования по составу и характеристикам подсистем защиты информации применительно к операционным системам Порядок реализации методов и средств антивирусной защиты в операционных системах Программно-аппаратные средства и методы защиты информации в операционных системах Принципы работы и правила эксплуатации программно-аппаратных средств защиты информации Нормативные правовые акты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Организационные меры по защите информации
	ИД-2.ПК-1 Уметь: Формулировать политики безопасности операционных систем Настраивать политики безопасности операционных систем Оценивать угрозы безопасности информации операционных систем Противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации операционных систем Выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах Настраивать антивирусные средства защиты информации в операционных системах Устанавливать обновления программного обеспечения и средств антивирусной защиты Проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах Производить анализ эффективности программно-аппаратных средств защиты информации в операционных системах Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах

ПК-1 Администрирование подсистем защиты информации в операционных системах	ИД-3.ПК-1 Иметь практический опыт: Определение состава применяемых программно-аппаратных средств защиты информации в операционных системах Разработка порядка применения программно-аппаратных средств защиты информации в операционных системах Формирование шаблонов установки программно-аппаратных средств защиты информации в операционных системах Установка программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации Конфигурирование программно-аппаратных средств защиты информации в операционных системах Контроль корректности функционирования программно-аппаратных средств защиты информации в операционных системах Управление антивирусной защитой операционных систем в соответствии с действующими требованиями
ПК-2 Администрирование программно-аппаратных средств защиты информации в компьютерных сетях	ИД-1.ПК-2 Знать: Принципы построения компьютерных сетей Стек сетевых протоколов операционных систем Стек протоколов сетевого оборудования Порядок реализации методов и средств межсетевого экранирования Принципы функционирования сетевых протоколов, включающих криптографические алгоритмы Виды политик управления доступом и информационными потоками в компьютерных сетях Источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению Состав типовых конфигураций программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях Методы измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации Принципы работы и правила эксплуатации эксплуатируемых программно-аппаратных средств защиты информации Программно-аппаратные средства и методы защиты информации в компьютерных сетях Нормативные правовые акты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Организационные меры по защите информации

ПК-2 Администрирование программно-аппаратных средств защиты информации в компьютерных сетях	ИД-2.ПК-2 Уметь: Оценивать угрозы безопасности информации в компьютерных сетях Настраивать правила фильтрации пакетов в компьютерных сетях Обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных сетях Конфигурировать и контролировать корректность настройки программно-аппаратных средств защиты информации в компьютерных сетях Выбирать режимы работы программно-аппаратных средств защиты информации в компьютерных сетях Проводить мониторинг функционирования программно-аппаратных средств защиты информации в компьютерных сетях Производить анализ эффективности программно-аппаратных средств защиты информации в компьютерных сетях Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях
	ИД-3.ПК-2 Иметь практический опыт: Определение состава применяемых программно-аппаратных средств защиты информации в компьютерных сетях Разработка порядка применения программно-аппаратных средств защиты информации в компьютерных сетях Формирование шаблонов конфигурации программно-аппаратных средств защиты информации в компьютерных сетях Настройка программных и аппаратных средств построения компьютерных сетей, использующих криптографическую защиту информации Управление функционированием программно-аппаратных средств защиты информации в компьютерных сетях Контроль корректности функционирования программно-аппаратных средств защиты информации в компьютерных сетях Управление средствами межсетевого экранирования в компьютерных сетях в соответствии с действующими требованиями

ПК-3 Подготовка данных для проведения аналитических работ по исследованию больших данных	ИД-1.ПК-3 Знать: Архитектура подсистем защиты информации в операционных системах Принципы построения систем управления базами данных Основные средства и методы анализа программных реализаций Принципы построения антивирусного программного обеспечения Виды политик управления доступом и информационными потоками применительно к прикладному программному обеспечению Источники угроз информационной безопасности программного обеспечения и меры по их предотвращению Уязвимости используемого программного обеспечения и методы их эксплуатации Виды и формы функционирования вредоносного программного обеспечения Характерные признаки наличия вредоносного программного обеспечения Средства и методы обнаружения ранее неизвестного вредоносного программного обеспечения Принципы функционирования программных средств криптографической защиты информации Порядок обеспечения безопасности информации при эксплуатации программного обеспечения Нормативные правовые акты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Организационные меры по защите информации
	ИД-2.ПК-3 Уметь: Анализировать угрозы безопасности информации программного обеспечения Формулировать правила безопасной эксплуатации программного обеспечения Обосновывать правила безопасной эксплуатации программного обеспечения Анализировать функционирование программного обеспечения с целью определения возможного вредоносного воздействия Производить проверку соответствия реальных характеристик программно-аппаратных средств защиты информации заявленным в их технической документации Осуществлять мероприятия по противодействию угрозам безопасности информации, возникающим при эксплуатации программного обеспечения Определять порядок функционирования программного обеспечения с целью обеспечения защиты информации Анализировать эффективность сформулированных требований к встроенным средствам защиты информации программного обеспечения

ПК-3 Подготовка данных для проведения аналитических работ по исследованию больших данных	ИД-3.ПК-3 Иметь практический опыт: Определение порядка установки программного обеспечения с целью соблюдения требований по защите информации Контроль над соблюдением требований по защите информации при установке программного обеспечения, включая антивирусное программное обеспечение Формулирование требований к параметрам средств антивирусной защиты для корректной работы программного обеспечения Выполнение работ по обнаружению вредоносного программного обеспечения Ликвидация обнаруженного вредоносного программного обеспечения и последствий его функционирования Формулирование требований к встроенным средствам защиты информации программного обеспечения

5. ТЕМАТИЧЕСКИЙ ПЛАН

Этап	Часов						
	Наименование этапа	Всего часов	Контактная работа .(по уч.зан.)			Самост. работа	Контроль самостоятельной работы
			Лекции	Лабораторные	Практические занятия		
Семестр 8		36					
Этап 1.	Работа с нормативными документами организации, знакомство с основными бизнес-процессами	36	2			34	
Семестр 8		80					
Этап 2.	Участие в осуществлении процедур информационно-аналитического мониторинга в сфере информационной безопасности конкретной организации	80				80	
Семестр 8		100					
Этап 3.	Реализация и внедрение модели информационно-аналитического мониторинга в сфере информационной безопасности и анализ результатов работы по проведенной процедуре.	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 - 3	Аналитическая записка	Структура данных по проблеме исследования, выводов, рекомендаций	Оценивается умение: - собрать данные (30%) - проанализировать данные (50%) - сделать выводы (20%) Процент выполнения: 0-100%
Промежуточный контроль			
8 семестр (За)	Отчет и приложение к отчету	Включает: характеристику места практики, приложения. Защита отчета: вопросы по аналитической справке	Оценивается: - правильность интерпретации данных по проблеме исследования (50%) - аргументированность выводов м предложений (50%) Процент выполнения: 0-100%

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 профессиональных задач
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. Работа с нормативными документами организации, знакомство с основными бизнес-процессами Проведение инструктажа на месте прохождения практики. Знакомство с руководителем, определение видов деятельности бакалавра на время прохождения практики.

7.3. Содержание самостоятельной работы

Этап 1. Работа с нормативными документами организации, знакомство с основными бизнес-процессами Совершенствование навыков использования современных средств и инструментов информационно-аналитического мониторинга в сфере информационной безопасности, работа с нормативными документами организации, знакомство с основными бизнес-процессами. Анализ инструментальных средств инструментов информационно-аналитического мониторинга в сфере информационной безопасности, используемых в организации. Анализ регламентов в сфере информационной безопасности организации. Работа с данными. Описание экосистемы информационно-аналитического мониторинга в организации
Этап 2. Участие в осуществлении процедур информационно-аналитического мониторинга в сфере информационной безопасности конкретной организации Участие в осуществлении процедур информационно-аналитического мониторинга в сфере информационной безопасности конкретной организации в соответствии с планом практики и поставленной индивидуальной задачей с помощью инструментальных средств, используемых в организации. Изучение проблем, "узких мест" в сфере информационной безопасности организации. Поиск и анализ научно-практического контента по проблеме. Обзор теоретических подходов по решению проблем. Выбор и описание методики решения конкретной задачи. Разработка модели решения задачи информационно-аналитического мониторинга в сфере информационной безопасности. Выполнение задания по поручению и под наблюдением специалиста по ИБ (руководителя или специалиста ИТ-отдела, инженера по ИБ).
Этап 3. Реализация и внедрение модели информационно-аналитического мониторинга в сфере информационной безопасности и анализ результатов работы по проведенной процедуре. Осуществление сбора, обработки, анализа и систематизации информации по проведенному научному обзору контента и методик, реализация процедуры в информационно-аналитического мониторинга в сфере информационной безопасности. Анализ инструментальных моделей информационно-аналитического мониторинга в сфере информационной безопасности. Разработка модели по индивидуальному заданию. Реализация модели с помощью инструментального средства информационно-аналитического мониторинга в сфере информационной безопасности и анализ результатов работы по проведенной процедуре. Внедрение разработанной модели в процесс информационно-аналитического мониторинга в сфере информационной безопасности 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
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. Космин В.В. Основы научных исследований (Общий курс). [Электронный ресурс]:Учебное пособие. - Москва: Издательский Центр РИОР, 2020. - 238 – Режим доступа: https://znanium.com/catalog/product/1088366

2. Усенко Л.Н., Чернышева Ю.Г. Бизнес-анализ деятельности организации [Электронный ресурс]:Учебник. - Москва: Издательский дом "Альфа-М", 2019. - 560 – Режим доступа: https://znanium.com/catalog/product/1003063

3. Ермолаев В. А. Введение в научно-исследовательскую деятельность [Электронный ресурс]:учебное пособие для студентов вузов. - Кемерово: КемГУ, 2017. - 69 с. – Режим доступа: https://e.lanbook.com/book/103931

4. Горелов Н. А., Круглов Д. В., Кораблева О. Н. Методология научных исследований. [Электронный ресурс]:Учебник и практикум для вузов. - Москва: Юрайт, 2020. - 365 – Режим доступа: https://urait.ru/bcode/450489

5. Шкляр М.Ф. Основы научных исследований [Электронный ресурс]:Учебное пособие для бакалавров. - Москва: Издательско-торговая корпорация "Дашков и К", 2019. - 208 с. – Режим доступа: https://znanium.com/catalog/product/1093533

6. Плутова Научно-исследовательская работа. Курс лекций. Лекция 2. Этапы выполнения НИ�[Электронный ресурс]:. - Екатеринбург: [б. и.], 2020. - 1 – Режим доступа: http://lib.wbstatic.usue.ru/202009/214.mp4

7. Плутова Научно-исследовательская работа. Курс лекций. Лекция 3. Методы в НИ� [Электронный ресурс]:. - Екатеринбург: [б. и.], 2020. - 1 – Режим доступа: http://lib.wbstatic.usue.ru/202009/215.mp4

Дополнительная литература:

1. Вейнберг Р.Р. Интеллектуальный анализ данных и систем управления бизнес-правилами в телекоммуникациях [Электронный ресурс]:Монография. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2016. - 173 с. – Режим доступа: https://znanium.com/catalog/product/520998

2. Сафронова Т.Н., Тимофеева А.М. Основы научных исследований: лаб. практикум для студентов направления подготовки 101100.62 «Гостиничное дело» профиля «Ресторанная деятельность» всех форм обучения [Электронный ресурс]:Учебное пособие. - Красноярск: Сибирский федеральный университет, 2015. - 131 с. – Режим доступа: https://znanium.com/catalog/product/550149

3. Пижурин А. А., Пижурин (мл.) А.А. Методы и средства научных исследований. [Электронный ресурс]:ВО - Бакалавриат. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2020. - 264 – Режим доступа: https://znanium.com/catalog/product/1085368

4. Буряк В.А., Лысенко Н.А. Аннотирование и реферирование научных и специализированных текстов [Электронный ресурс]:Учебное пособие. - Москва: Российский государственный университет правосудия, 2019. - 100 с. – Режим доступа: https://znanium.com/catalog/product/1190650

5. Тихонов В. А., Ворона В. А. Научные исследования : концептуальные, теоретические и практические аспекты:[учебное пособие для вузов]. - Москва: Горячая линия - Телеком, 2013. - 296

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. Договор № 1 от 13 июня 2018, акт от 17 декабря 2018. Срок действия лицензии - без ограничения срока.

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

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

IBLite XE7. Эл. лицензия, Информационное письмо.

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

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

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

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

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

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

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

Справочно-правовая система Консультант +. Срок действия лицензии до 31.12.2023

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

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.