

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Сенченко Павел Васильевич
Должность: Проректор по учебной работе
Дата подписания: 27.09.2023 08:59:24
Уникальный программный ключ:
27e516f4c088deb62ba68945f4406e13fd454355

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ» (ТУСУР)

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ПРАКТИКИ

ПРОИЗВОДСТВЕННАЯ ПРАКТИКА: ЭКСПЛУАТАЦИОННАЯ ПРАКТИКА

Уровень образования: **высшее образование - магистратура**

Направление подготовки / специальность: **10.04.01 Информационная безопасность**

Направленность (профиль) / специализация: **Информационная безопасность объектов критической информационной инфраструктуры**

Форма обучения: **очная**

Факультет: **Факультет безопасности (ФБ)**

Кафедра: **Кафедра комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС)**

Курс: **1**

Семестр: **2**

Количество недель: **4**

Учебный план набора 2023 года

Объем практики и виды учебной деятельности

Виды учебной деятельности	2 семестр	Всего	Единицы
Контактная работа	48	48	часов
в т.ч. в форме практической подготовки	48	48	часов
Иные формы работ	168	168	часов
в т.ч. в форме практической подготовки	168	168	часов
Общая трудоемкость	216	216	часов
(включая промежуточную аттестацию)	6	6	з.е.

Формы промежуточной аттестация	Семестр
Зачет с оценкой	2

1. Общие положения

Производственная практика: эксплуатационная практика (далее – практика) в соответствии с ФГОС ВО по направлению подготовки / специальности 10.04.01 Информационная безопасность является формой практической подготовки и обязательным этапом в процессе освоения обучающимися основной образовательной программы.

Вид практики: производственная практика.

Тип практики: эксплуатационная практика.

Практика представляет собой вид учебных занятий, непосредственно ориентированных на научно-исследовательскую подготовку.

Место практики в структуре ОПОП:

Блок практик: Б2. Практика.

Часть блока практик: Часть, формируемая участниками образовательных отношений.

Индекс практики: Б2.В.1(П).

При реализации практики могут применяться электронное обучение, дистанционные образовательные технологии. Практика проводится в соответствии с утвержденным учебным планом и рабочим календарным учебным графиком.

Объем практики в зачетных единицах и ее продолжительность в неделях либо в академических или астрономических часах: продолжительность, сроки прохождения и объем практики в зачетных единицах определяются учебным планом в соответствии с ФГОС ВО по направлению подготовки / специальности 10.04.01 Информационная безопасность. Общая трудоемкость данной практики составляет 6 з.е., количество недель: 4 (216 часов).

Форма проведения практики: дискретно по видам практик – путем выделения в календарном учебном графике непрерывного периода учебного времени для проведения каждой практики.

Основной формой прохождения практики является непосредственное участие обучающегося в производственном процессе конкретной организации..

2. Цели и задачи практики

2.1. Цели практики

Углубление и закрепление знаний и умений, полученных студентом при теоретическом обучении в университете, расширение технического кругозора студента, приобретение студентом навыков работы по направлению подготовки, подготовка студента к самостоятельной специальной деятельности, приобретение опыта организаторской и руководящей работы..

2.2. Задачи практики

- ознакомление со структурой подразделения, в котором проходит практика, его функциями и связями с другими подразделениями предприятия;
- изучение организации проектных работ;
- приобретение практических навыков на рабочем месте специалиста по защите информации;
- ознакомление с видами документации, стандартами, нормами и т.п.;
- закрепление знаний и выработка умений по проектированию средств защиты информации, составлению и использованию программного обеспечения и т.п.;
- выработка умений и навыков при работе на автоматизированном рабочем месте;
- выработка навыков творческого подхода к решению теоретических и практических задач по направлению подготовки;
- пополнение знаний по безопасности жизнедеятельности.

3. Перечень планируемых результатов обучения при прохождении практики, соотнесенных с индикаторами достижения компетенций

Процесс прохождения практики направлен на поэтапное формирование и закрепление следующих компетенций (таблица 3.1):

Таблица 3.1 – Компетенции и индикаторы их достижения

Компетенция	Индикаторы достижения компетенции
Универсальные компетенции	

УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1. Знает методики сбора и обработки информации, актуальные российские и зарубежные источники информации для решения поставленных задач, а также методы системного анализа
	УК-1.2. Умеет применять методики поиска, сбора и обработки информации, осуществлять критический анализ и синтез информации, полученной из разных источников
	УК-1.3. Владеет методами поиска, сбора и обработки, критического анализа и синтеза информации, методикой системного подхода для решения поставленных задач; способен генерировать различные варианты решения поставленных задач
УК-2. Способен управлять проектом на всех этапах его жизненного цикла	УК-2.1. Знает основные модели жизненного цикла проекта, его этапы и фазы, их характеристики и особенности
	УК-2.2. Умеет разрабатывать и реализовывать этапы проекта в сфере профессиональной деятельности
	УК-2.3. Имеет навыки работы в области проектной деятельности и реализации проектов
Общепрофессиональные компетенции	
-	-
Профессиональные компетенции	
ПК-1. Способен обеспечивать анализ, проектирование, разработку, функционирование, эксплуатацию систем информационной безопасности объектов критической информационной инфраструктуры и ее частей;	ПК-1.1. Знает общие принципы проектирования систем информационной безопасности объектов критической информационной инфраструктуры и ее частей, принципы построения систем информационной безопасности объектов критической информационной инфраструктуры и ее частей, состав технико-экономического обоснования проектируемых систем информационной безопасности объектов критической информационной инфраструктуры и ее частей
	ПК-1.2. Умеет разрабатывать необходимую техническую документацию в области проектирования систем информационной безопасности объектов критической информационной инфраструктуры и ее частей с учетом действующих нормативных и методических документов, проводить подготовку исходных данных для технико-экономического обоснования проектируемых систем информационной безопасности объектов критической информационной инфраструктуры и ее частей
	ПК-1.3. Владеет навыками проектирования элементов систем информационной безопасности объектов критической информационной инфраструктуры
ПК-2. Способен осуществлять разработку проектных решений по защите информации на объектах критической информационной инфраструктуры;	ПК-2.1. Знает основные угрозы безопасности информации и модели нарушителя в системах информационной безопасности объектов критической информационной инфраструктуры
	ПК-2.2. Знает методы и инструменты проведения исследований в ходе проектной деятельности
	ПК-2.3. Умеет проводить анализ проектных решений при проектировании и исследовании систем информационной безопасности объектов критической информационной инфраструктуры
	ПК-2.4. Умеет определять структуру системы защиты информации систем информационной безопасности объектов критической информационной инфраструктуры в соответствии с требованиями нормативных правовых документов в области защиты информации

ПК-3. Способен разрабатывать организационно-распорядительные документы, регламентирующие функционирование систем информационной безопасности объектов критической информационной инфраструктуры	ПК-3.1. Знает содержание и порядок деятельности персонала по эксплуатации систем информационной безопасности объектов критической информационной инфраструктуры
	ПК-3.2. Знает нормативную базу, регламентирующую процессы проектирования, построения и эксплуатации систем информационной безопасности объектов критической информационной инфраструктуры
	ПК-3.3. Умеет разрабатывать технические задания на создание систем информационной безопасности объектов критической информационной инфраструктуры с учетом действующих нормативных и методических документов
	ПК-3.4. Владеет инструментами проведения и фиксации результатов проверки функционирования систем информационной безопасности объектов критической информационной инфраструктуры
	ПК-3.5. Умеет осуществлять планирование и организацию работы персонала систем информационной безопасности объектов критической информационной инфраструктуры с учетом требований по защите информации.

4. Структура и содержание практики

Прохождение практики осуществляется в три этапа:

1. Подготовительный этап (проведение инструктивного совещания, ознакомление обучающихся с содержанием и спецификой деятельности организации, доведение до обучающихся заданий на практику, видов отчетности по практике).

2. Основной этап (выполнение обучающимися заданий, их участие в различных видах профессиональной деятельности согласно направлению подготовки / специальности). Выбор конкретных заданий определяется совместно с руководителем практики от организации.

3. Завершающий этап (оформление и сдача обучающимися отчета о выполнении индивидуальных заданий по практике и дневника, анализ проделанной работы и подведение её итогов).