

Документ подписан электронной подписью
Информация о владельце:
ФИО: Сенченко Павел Васильевич
Должность: Проректор по учебной работе
Дата подписания: 25.10.2023 08:18:00
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:
ПРЕДДИПЛОМНАЯ ПРАКТИКА**

Уровень образования: **высшее образование - бакалавриат**

Направление подготовки / специальность: **10.03.01 Информационная безопасность**

Направленность (профиль) / специализация: **Безопасность автоматизированных систем**

Форма обучения: **очная**

Факультет: **ФБ, Факультет безопасности**

Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**

Курс: **4**

Семестр: **8**

Количество недель: **10**

Учебный план набора 2020 года

Распределение рабочего времени

Виды учебной деятельности	8 семестр	Всего	Единицы
1. Контактная работа	15	15	часов
2. Иные формы работ	525	525	часов
3. Общая трудоемкость	540	540	часов
	15.0	15.0	З.Е.

Зачёт с оценкой: 8 семестр

Томск

1. ОБЩИЕ ПОЛОЖЕНИЯ

Производственная практика: Преддипломная практика (далее практика) в соответствии с ФГОС ВО подготовки бакалавров по направлению 10.03.01 Информационная безопасность является обязательным этапом в процессе освоения обучающимися образовательной программы.

Вид практики: Производственная практика.

Тип практики: Преддипломная практика (практика проводится для выполнения выпускной квалификационной работы и является обязательной).

Практика представляет собой вид учебных занятий, непосредственно ориентированных на профессионально-практическую подготовку обучающихся..

Место практики в структуре образовательной программы: данная практика входит в блок 2. Практика проводится в соответствии с утвержденным рабочим учебным планом и календарным учебным графиком.

Практике предшествуют дисциплины: «Безопасность операционных систем», «Дискретная математика», «Криптографические методы защиты информации», «Методы оптимизации», «Организационное и правовое обеспечение информационной безопасности», «Основы информационной безопасности», «Основы программирования», «Прикладная криптография», «Системный анализ», «Теория вероятностей и математическая статистика», «Техническая защита информации», «Численные методы», «Языки программирования».

Данная практика является основой для более глубокого усвоения обучающимися следующих дисциплин: «Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты».

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) 10.03.01 Информационная безопасность. Общая трудоемкость данной практики составляет 15.0 З.Е., количество недель: 10. (540 часов).

Способы проведения практики: стационарная, выездная.

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. ЦЕЛЬ И ЗАДАЧИ ПРАКТИКИ

Цель практики: выполнение ВКР; углубление и закрепление знаний и умений, полученных студентом при теоретическом обучении в университете; расширение технического кругозора студента; приобретение студентом навыков работы по специальности; подготовка студента к самостоятельной специальной деятельности;

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;;
- формулирование совместно с руководителем темы дипломного проекта (работы) и подготовка к его выполнению;;
- выработка навыков творческого подхода к решению теоретических и практических задач по специальности;;

- сбор материалов, необходимых для выполнения выпускной квалификационной работы;;
- выработка умений оценки технико-экономических показателей выполняемой выпускной квалификационной работы в соответствии с действующими нормативно-техническими документами;;
- пополнение знаний по безопасности жизнедеятельности..

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПРИ ПРОХОЖДЕНИИ ПРАКТИКИ

Процесс прохождения практики направлен на поэтапное формирование и закрепление следующих компетенций:

- способностью использовать основы философских знаний для формирования мировоззренческой позиции (ОК-1);
- способностью использовать основы экономических знаний в различных сферах деятельности (ОК-2);
- способностью анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма (ОК-3);
- способностью использовать основы правовых знаний в различных сферах деятельности (ОК-4);
- способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-5);
- способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия (ОК-6);
- способностью к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности (ОК-7);
- способностью к самоорганизации и самообразованию (ОК-8);
- способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности (ОК-9);
- способностью анализировать физические явления и процессы для решения профессиональных задач (ОПК-1);
- способностью применять соответствующий математический аппарат для решения профессиональных задач (ОПК-2);
- способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач (ОПК-3);
- способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации (ОПК-4);
- способностью использовать нормативные правовые акты в профессиональной деятельности (ОПК-5);
- способностью применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности (ОПК-6);
- 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 (ОПК-7);
- способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1);
- способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10);
- способностью проводить эксперименты по заданной методике, обработку, оценку по-

грешности и достоверности их результатов (ПК-11);

– способностью принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12);

– способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации (ПК-13);

– способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности (ПК-14);

– 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 (ПК-15);

– способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2);

– способностью администрировать подсистемы информационной безопасности объекта защиты (ПК-3);

– способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4);

– способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5);

– способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6);

– способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-7);

– способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов (ПК-8);

– 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 (ПК-9);

– способностью создавать и исследовать модели автоматизированных систем (ПСК-4.1);

– способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем (ПСК-4.2).

В результате прохождения практики обучающийся должен:

– **знать** основные методы проведения научно-исследовательской деятельности, необходимой для выполнения выпускной квалификационной работы;

– **уметь** на практике применять навыки, полученные при изучении всех предыдущих дисциплин для решения научно-исследовательских задач и производственных по направлению подготовки, составлять детальный план проводимого исследования; – отбирать и анализировать необходимую информацию по теме исследования, готовить аналитический обзор; – формулировать выводы исследования, оформлять законченные проектно-конструкторские работы. ;

– **владеть** – общими методами научных исследований, включая теоретические и экспериментальные методы моделирования..

4. СОДЕРЖАНИЕ ПРАКТИКИ

Практика 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 про-

фессиональной деятельности согласно направлению подготовки). Выбор конкретных заданий определяется совместно с руководителем практики от организации.

3. *Завершающий этап* (оформление обучающимися отчета о выполнении индивидуальных заданий по практике, анализ проделанной работы и подведение её итогов, публичная защита отчета по практике на основе презентации обучающимися перед комиссией с приглашением работодателей и руководителей от университета, оценивающих результативность практики).