МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

Рабочая программа практики,
как компонент образовательной программы
высшего образования - программа специалитета
по специальности
10.05.01 Компьютерная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

Производственная практика

Технологическая практика

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Информационная безопасность объектов информатизации на базе компьютерных систем

Форма обучения: Очная

Рабочая программа практики в виде электронного документа выгружена из единой корпоративной информационной системы управления университетом и соответствует оригиналу

Простая электронная подпись, выданная РУТ (МИИТ)
ID подписи: 2053
Подписал: заведующий кафедрой Баранов Леонид Аврамович
Дата: 01.06.2022

1. Общие сведения о практике.

Практика проводится для реализации контрольно-аналитического и организационно-управленческого видов профессиональной деятельности. Основной целью практики по получению профессиональнальных умений и опыта профессиональной деятельности студентов является закрепление и углубление теоретических знаний и умений по специальности, получение практического опыта самостоятельного решения производственных задач, изучение технологии изготовления, отладки и испытаний основных программно-аппаратных средств защиты информации. На практике студент должен закрепить и углубить теоретические знания, полученные в университете. Он должен приобрести практические опыт и умения профессиональной деятельности. В цели практики входит глубокое и всестороннее изучение наиболее передовой технологии защиты информации и зависимости от конкретных условий. Наряду с этим, студентом должны быть изучены на производстве вопросы организации, планирования, экономики производства, вопросы организации труда и его охраны. Каждый студент должен принимать активное участие в общественных мероприятиях, проводимых на предприятии.

Задачами практики по получению профессиональных умений и опыта профессиональной деятельности являются: • научить применять на практике требования по защите информации нормативных правовых актов Российской Федерации. • развить способность анализировать безопасность компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности на примере реальных компьютерных систем, используемых на предприятии • развить способности творческого мышления студентов через разработку и анализ на выявление уязвимостей математических моделей реальных компьютерных систем; • сформировать умения и навыки по проведению экспериментально-исследовательских работ при аттестации объектов с учетом требований к уровню защищенности компьютерной системы

2. Способ проведение практики:

стационарная и (или) выездная

3. Форма проведения практики.

Практика проводится в форме практической подготовки.

При проведении практики практическая подготовка организуется путем непосредственного выполнения обучающимися определенных видов работ, связанных с будущей профессиональной деятельностью.

4. Организация практики.

Практика может быть организована:

- непосредственно в РУТ (МИИТ), в том числе в структурном подразделении РУТ (МИИТ);
- в организации, осуществляющей деятельность по профилю образовательной программы (далее - профильная организация), в том числе в структурном подразделении профильной организации, на основании договора, заключаемого между РУТ (МИИТ) и профильной организацией.

5. Планируемые результаты обучения при прохождении практики.

Перечень формируемых результатов освоения образовательной программы (компетенций) в результате обучения при прохождении практики:

ПК-9 - Способен участвовать в управлении информационной безопасностью компьютерной системы, разрабатывать предложения по ее совершенствованию;

ПК-10 - Способен организовать процесс защиты информации в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

ПК-20 - Способен подготовить обоснование необходимости защиты информации в автоматизированной системе.

Обучение при прохождении практики предполагает, что по его результатам обучающийся будет:

Уметь: ПК-9 Разрабатывает и организует выполнение мероприятий в соответствии с положениями политики информационной безопасности и защиты информации ограниченного доступа.

Уметь: ПК-9 Разрабатывать проекты нормативных правовых актов и методические материалы, регламентирующие работу по обеспечению информационной безопасности компьютерных систем.

Уметь: ПК-10 Проверяет уровень квалификации, распределяет полномочия и контролирует выполнение инструкций в отношении персонала

обслуживающего технические, программные и программно-аппаратные средства защиты информации.

Уметь: ПК-10 Анализирует компьютерные системы в сфере профессиональной деятельности с целью выявления условий, способствующих совершению правонарушений в отношении сведений ограниченного доступа.

Уметь: ПК-20 Проводит анализ уязвимости и устанавливает необходимые средства защиты информации для технологической базы автоматизированных систем высокоскоростного транспорта.

Уметь: ПК-20 Проводит анализ уязвимости и устанавливает необходимые средства защиты информации для технологической базы беспилотных автоматизированных систем.

6. Объем практики.

Объем практики составляет 5 зачетных единиц (180 академических часов).

7. Содержание практики.

Обучающиеся в период прохождения практики выполняют индивидуальные задания руководителя практики.

№ п/п	Краткое содержание
1	Подготовительный Вводный инструктаж на месте практики, инструктаж по охране труда и противопожарной безопасности
2	Выполнение производственных заданий на месте практики, сбор и обработка фактического материала
3	Обработка и анализ полученного материала
4	Подготовка отчета по практике
5	Защита отчета по практике

8. Перечень изданий, которые рекомендуется использовать при прохождении практики.

№ п/п	Библиографическое описание	Место доступа
1	Средства защиты информации на железнодорожном транспорте (Криптографические методы и средства) А.А. Корниенко, М.А. Еремеев, С.Е. Ададуров; Ред. А.А. Корниенко; Под Ред. А.А. Корниенко Однотомное издание Маршрут , 2006	НТБ (ЭЭ); НТБ (уч.3); НТБ (фб.); НТБ (чз.2)

2	Методы предотвращения и обнаружения вторжений В.П. Соловьев, Н.В. Павленко, Н.Н. Пуцко; Ред. В.П. Соловьев; МИИТ. Центр компетентности "Защита и безопасность информации" Однотомное издание МИИТ , 2007	НТБ (ЭЭ); НТБ (фб.); НТБ (чз.2)
3	Комплексная система защиты информации на предприятии А.Г. Лихоносов Юридический институт МИИТа. ИТБ УЛУПС (Абонемент ЮИ) , 2011	
4	Основы информационной безопасности и защиты сведений, составляющих, государственную тайну В.Н. Кухарев Юридический институт МИИТа. ИТБ УЛУПС (Абонемент ЮИ) , 2005	
1	Информационная безопасность и защита информации В.П. Мельников, С.А. Клейменов, А.М. Петраков Книга Издательский центр "Академия" , 2011	ИТБ УЛУПС (Абонемент ЮИ); ИТБ УЛУПС (ЧЗ1 ЮИ)
2	Модели безопасности компьютерных систем П.Н. Девянин Однотомное издание Академия , 2005	НТБ (фб.)

9. Форма промежуточной аттестации: Дифференцированный зачет в 6 семестре

10. Оценочные материалы.

Оценочные материалы, применяемые при проведении промежуточной аттестации, разрабатываются в соответствии с локальным нормативным актом РУТ (МИИТ).

Авторы:

профессор, профессор, д.н. кафедры «Управление и защита информации» В.М. Алексеев

А.В. Ваганов

Согласовано:

Заведующий кафедрой УиЗИ Л.А. Баранов

Председатель учебно-методической комиссии С.В. Володин