

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 - программы 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: 01.06.2025

1. Общие сведения о практике.

Практика проводится для реализации контрольно-аналитического и организационно-управленческого видов профессиональной деятельности. Основной целью практики по получению профессиональных 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 практический 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 проведения 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:

Знать: - Методы управления информационной безопасностью компьютерной системы и подходы к разработке предложений по ее совершенствованию.

- Нормативные правовые акты и нормативные методические документы Федеральной службы безопасности Российской Федерации и Федеральной службы по техническому и экспортному контролю.

- Методические основы и критерии для подготовки обоснования необходимости защиты информации в автоматизированной системе.

Уметь: - Разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы.

- Организовывать процесс защиты информации в соответствии с требованиями нормативных правовых актов и методических документов ФСБ и ФСТЭК России.
- Подготавливать обоснование необходимости защиты информации в автоматизированной системе.
- Разрабатывать проекты нормативных правовых актов и методические материалы, регламентирующие работу по обеспечению информационной безопасности компьютерных систем.
- Проверять уровень квалификации, распределять полномочия и контролировать выполнение инструкций персоналом, обслуживающим средства защиты информации.
- Анализировать компьютерные системы с целью выявления условий, способствующих совершению правонарушений в отношении сведений ограниченного доступа.

Владеть: - Навыками разработки и организации выполнения мероприятий в соответствии с положениями политики информационной безопасности и защиты информации ограниченного доступа.

- Навыками анализа уязвимостей и определения необходимых средств защиты информации для технологической базы автоматизированных систем (в т.ч. высокоскоростного транспорта).
- Навыками анализа уязвимостей и определения необходимых средств защиты информации для технологической базы беспилотных автоматизированных систем.

6. Объем практики.

Объем практики составляет 6 зачетных единиц (216 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

№ п/п	Краткое содержание
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	Программно-аппаратные средства защиты информации Зырянов С. А., Кувшинов М. А., Огнев И. А., Никрошкин И. В. Учебное пособие — Новосибирск : НГТУ, - 80 с., — ISBN 978-5-7782-4905-9. , 2023	https://reader.lanbook.com/book/404549#2
2	Криптографические протоколы Корниенко А. А., Глухарев М. Л. Учебное пособие Санкт-Петербург: ПГУПС, 76 с., — ISBN 978-5-7641-1509-2. , 2020	https://reader.lanbook.com/book/191009#2
3	Защита информации Груздева Л. М. Учебное пособие М.: Российский университет транспорта, - 144 с. - ISBN 978-5-7876-0326-2 , 2019	https://reader.lanbook.com/book/188703

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

Согласовано:

Заведующий кафедрой УиЗИ

Л.А. Баранов

Председатель учебно-методической
комиссии

С.В. Володин