

**МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ**  
**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ**  
**УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**  
**«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»**  
**(РУТ (МИИТ))**



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

## **РАБОЧАЯ ПРОГРАММА ПРАКТИКИ**

### **Производственная практика**

### **Научно-исследовательская работа**

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: 01.06.2026

## 1. Общие сведения о практике.

Целями практики являются получение и развитие компетенций научно-исследовательской деятельности.

В соответствии с целями ОП ВО «Научно-исследовательская работа» направлена формирование у будущих специалистов умения самостоятельно вести научно-исследовательскую деятельность и позволяет:

- повысить качество подготовки выпускников в университете как едином учебно-научно-производственном комплексе через освоение студентами в процессе обучения по учебным планам и сверх них основ профессионально-творческой деятельности;

- закрепление и углубление теоретической подготовки обучающегося, приобретение им практических навыков и компетенций, а также опыта самостоятельной профессиональной деятельности.

Задачами практики являются :

- способности к самостоятельному обучению новым методам исследования, к изменению научного и научно-производственного профиля своей профессиональной деятельности;

- способности самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения, в том числе в новых областях знаний, непосредственно не связанных со сферой деятельности;

- способности проектировать сложные системы и комплексы управления информационной безопасностью с учетом особенностей объектов защиты;

- способности разработать программы и методики испытаний, организовать тестирование и отладку программно- аппаратных, криптографических и технических систем и средств обеспечения информационной безопасности.

НИР выполняется каждым студентом индивидуально на тему, выдаваемую научным руководителем (или выбираемую совместно с научным руководителем) и утверждаемую кафедрой. Тема НИР должна быть актуальной и соответствовать специальности и уровню учебной подготовки студентов. Работа должна обладать тематической и логической завершенностью. Работа должна быть направлена на решение теоретической, методической либо практической задачи, результаты которой могут принести пользу для деятельности организаций, предприятий, учреждений, ведущих работы по направлению «Информационная безопасность», в научно-исследовательских, опытно-конструкторских либо учебно-методических работах, выполняемых на кафедре "Управление и защита информации".

Темы для научно-исследовательской работы:

Построение систем цифровых водяных знаков ЦВЗ в системах документооборота.

Цифровая подпись на основе использования эллиптических кривых в компьютерных системах.

Методы стеганографии для защиты информации в компьютерных системах.

Разработка лабораторных работ на тему «Криптография с открытым ключом». Методы квантовой криптографии для защиты информации в компьютерных системах.

Разработка и применение программно-аппаратных и инженерно-технических средств защиты информации, обеспечение информационной безопасности автоматизированных систем для высокоскоростного транспорта.

Разработка модели безопасности и мониторинга компьютерных сетей предприятий промышленного комплекса России.

Разработка комплексной системы защиты информации в корпоративных сетях.

Разработка политики безопасности в беспроводных сетях (WLAN).

Построение Web-приложений с учетом возможных методов нападения.

Разработка системы мониторинга информационной безопасности Web-приложений.

Защита информации и приложений с использованием удостоверяющих центров.

Разработка систем мониторинга компьютерной сети на основе методов распознавания.

Методы анализа протоколов для нахождения атак в сетевом трафике.

Методы анализа поведения пользователей в сети и выявление вредоносного поведения.

Разработка и анализ антивирусной защиты компьютерных сетей.

Разработка методов защиты почтовых приложений от спама.

Защита персональных данных и коммерческой тайны в компьютерных системах.

Разработка защиты информации в распределенных компьютерных системах.

Разработка защищённых баз данных.

Разработка системы информационной безопасности банков.

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:

**ОПК-2** - Способен понимать устройство и историю развития транспортной системы;

**ОПК-3** - Способен на основании совокупности математических методов, физических законов и моделей разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности;

**ОПК-4** - Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;

**ОПК-5** - Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ;

**ОПК-6** - Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей.

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

- Знать:** - Нормативные правовые акты и методическую документацию РФ в сфере информационной безопасности.
- Отечественный и зарубежный опыт по проблемам компьютерной безопасности.
  - Математические методы, применяемые в области компьютерной безопасности.
  - Методологию анализа исходных данных и формирования требований к компонентам систем защиты информации.
  - Принципы и методы разработки программно-аппаратных средств защиты информации, защищенных ОС, СУБД, сетей.
  - Основы комплексного подхода к обеспечению информационной безопасности объекта защиты.
  - Критерии и методики оценки эффективности систем защиты информации и политик безопасности.
  - Порядок организации и сопровождения аттестации объектов информатизации.
  - Методы и средства инструментального мониторинга защищенности компьютерных систем.
  - Основы управления информационной безопасностью компьютерной системы.
  - Методы и средства восстановления работоспособности подсистем защиты информации.
  - Методологию разработки моделей угроз, планов мероприятий и требований по защите информации.
  - Принципы создания системы защиты информации процессов проектирования, создания и модернизации объектов информатизации.
  - Требования к разработке проектов нормативных правовых актов и методических документов в области защиты информации.

- Уметь:** - Принимать участие в теоретических и экспериментальных исследованиях систем защиты информации.
- Применять математические методы, включая криптографические, для анализа и разработки защищенных компьютерных систем.
  - Проводить анализ исходных данных и формировать требования к компонентам и методам обеспечения информационной безопасности.
  - Участвовать в разработке подсистем информационной безопасности компьютерных систем.
  - Участвовать в проектировании и реализации комплексной защиты объекта информатизации.
  - Проводить оценку эффективности реализации систем защиты информации и

- действующих политик безопасности.
- Проводить анализ информационной безопасности объектов и систем для целей аттестации.
  - Проводить инструментальный мониторинг защищенности компьютерных систем.
  - Разрабатывать предложения по совершенствованию управления информационной безопасностью.
  - Организовывать процесс защиты информации в соответствии с требованиями ФСБ и ФСТЭК.
  - Выполнять работы по восстановлению работоспособности средств и подсистем защиты информации.
  - Реализовывать частные политики информационной безопасности и проводить мониторинг их эффективности.
  - Разрабатывать модели угроз и формировать требования по защите информации.
  - Разрабатывать планы мероприятий по защите информации.
  - Участвовать в создании системы защиты информации процессов проектирования, создания и модернизации.
  - Разрабатывать проекты нормативных правовых актов и методических документов в области защиты информации.

- Владеть:**
- Навыками сбора, обработки и анализа научно-технической информации по проблемам компьютерной безопасности.
  - Навыками применения математических методов для решения задач обеспечения компьютерной безопасности.
  - Навыками анализа исходных данных и формирования требований к подсистемам и средствам защиты информации.
  - Навыками разработки программно-аппаратных компонентов систем защиты информации.
  - Навыками реализации комплексного подхода к обеспечению информационной безопасности.
  - Навыками проверки эффективности систем защиты информации и политик безопасности.
  - Навыками анализа информационной безопасности объектов в рамках аттестационных работ.
  - Навыками использования инструментальных средств мониторинга защищенности компьютерных систем.
  - Навыками управления информационной безопасностью компьютерной системы.
  - Навыками организации процесса защиты информации в соответствии с

- нормативными требованиями.
- Навыками восстановления работоспособности программно-аппаратных средств защиты информации.
  - Навыками разработки моделей угроз и планов мероприятий по защите информации.
  - Навыками анализа эффективности систем защиты информации.
  - Навыками создания и интеграции систем защиты информации в процессы проектирования и модернизации.
  - Навыками разработки нормативной правовой и методической документации в области защиты информации.

#### 6. Объем практики.

Объем практики составляет 9 зачетных единиц (324 академических часов).

#### 7. Содержание практики.

Обучающиеся в период прохождения практики выполняют индивидуальные задания руководителя практики.

№ п/п	Краткое содержание
1	Этап: Постановка цели и задач исследований Проведение инструктажа по технике безопасности и охране труда в организации (структурном подразделении) — месте прохождения практики. Ознакомление с правилами внутреннего распорядка. Получение индивидуального задания от руководителя практики. Постановка цели и задач исследования. Составление плана работ на период практики.
2	Этап: Рациональные приемы поиска научно - технической информации Изучение и анализ научно-технической литературы, нормативных и методических документов по теме исследования. Освоение рациональных приемов поиска, сбора и обработки научно-технической информации. Проведение теоретических и экспериментальных исследований в области защиты информации в соответствии с темой индивидуального задания. Выполнение работ по оценке защищенности, моделированию, разработке или анализу компонентов систем защиты информации.
3	Этап: Исследования в области защиты информации, связанные с темой дипломной работы Обработка и анализ полученных результатов. Формулирование выводов и рекомендаций по результатам выполненного исследования. Подготовка отчета о прохождении практики. Представление отчета и защита результатов руководителю практики (дифференцированный зачет).

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

№ п/п	Библиографическое описание	Место доступа
1	Управление информационной безопасностью Давыдов А.И., Елизаров Д.А. Учебное пособие Омский гос. ун-т путей сообщения, Омск, - 91 с. , 2023	<a href="https://reader.lanbook.com/book/419255#3">https://reader.lanbook.com/book/419255#3</a>
2	Введение в информационную безопасность: основы, методы, задачи: практикум Садыков А. М., Касимова А. Р., Алексеева А. А.В. Учебное пособие — Казань : КНИТУ, 92 с. — ISBN 978-5-7882-3573-8. , 2024	<a href="https://reader.lanbook.com/book/513551#2">https://reader.lanbook.com/book/513551#2</a>
3	Программно-аппаратные средства защиты информации Маршаков Д. В., Фатхи Д. В. Учебное пособие Ростов-на-Дону : Донской ГТУ, - 229 с. — ISBN 978-5-7890-1878-1. , 2021	<a href="https://reader.lanbook.com/book/237770#3">https://reader.lanbook.com/book/237770#3</a>
4	Методы защиты информации Краковский Ю. М. Учебное пособие 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — ISBN 978-5-8114-5632-1. , 2021	<a href="https://reader.lanbook.com/book/156401#1">https://reader.lanbook.com/book/156401#1</a>

9. Форма промежуточной аттестации: Дифференцированный зачет в 11 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  
"Интеллектуальное управление и  
информационная безопасность в  
высокоавтоматизированных  
транспортных системах" Института  
железнодорожного транспорта

В.М. Алексеев

Согласовано:

Заведующий кафедрой УиЗИ

Л.А. Баранов

Председатель учебно-методической  
комиссии

С.В. Володин