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 ФГАОУ ВО
РУТ (МИИТ) Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

Производственная практика

Эксплуатационная 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 ФГАОУ ВО РУТ (МИИТ)
ID подписи: 2053
Подписал: заведующий кафедрой Баранов Леонид Аврамович
Дата: 01.09.2026

1. Общие сведения о практике.

Эксплуатационная практика предназначена для получения практических знаний, умений и навыков, необходимых для решения профессиональных задач. Основной целью практики является формирование у обучающегося компетенций для эксплуатационного вида деятельности, а также в области профессиональной специализации №8 "Информационная безопасность объектов информатизации на базе компьютерных систем".

Целями эксплуатационной практики являются:

- закрепление теоретических знаний и умений, а также получение практического опыта в области проектирования и исследования средств и систем защиты информации на выявление уязвимостей;

- формирование следующих профессиональных компетенций:

- способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем;

- способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации;

- способность проводить инструментальный мониторинг защищенности компьютерных систем;

- способность организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности;

- способность организовывать работы по выполнению режима защиты информации, в том числе ограниченного доступа;

- способность производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение;

- способность производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации;

- способность производить проверки технического состояния и профилактические осмотры технических средств защиты информации;

- способность выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций.

Задачами эксплуатационной практики является:

• развить способности творческого мышления студентов через разработку и анализ на выявление уязвимостей математических моделей реальных компьютерных систем;

• научить студентов грамотно эксплуатировать, разрабатывать и конфигурировать

реальные средства защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации;

• сформировать умения и навыки по выявлению утечек информации путем инструментального мониторинга компьютерных систем, используемых на предприятии;

• закрепить теоретические знания и умения студентов опытом практической работы по проверке технического состояния, проведению профилактических осмотров и восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций;

• научить применять на практике требования по защите информации нормативных правовых актов Российской Федерации.

• развить организаторские способности студентов и способность находить и принимать управленческие решения в сфере профессиональной деятельности, а также способность организовывать работы по выполнению режима защиты информации, в том числе ограниченного доступа, путем формирования из них малых коллективов исполнителей, направленных на решение общей задачи.

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:

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

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;

УК-3 - Способен организовать работу команды для достижения поставленной цели;

УК-8 - Способен создавать и поддерживать безопасные условия жизнедеятельности, в том числе при угрозе и возникновении чрезвычайных ситуаций.

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

Знать: - Методологию проведения теоретических и экспериментальных исследований систем защиты информации.
- Математические методы, применяемые в области компьютерной безопасности.
- Методологию анализа исходных данных и формирования требований к компонентам и методам обеспечения информационной безопасности.
- Принципы и методы разработки программно-аппаратных средств защиты информации, защищенных ОС, СУБД, сетей, антивирусных и криптографических средств.

- Основы комплексного подхода к обеспечению информационной безопасности объекта защиты.
- Критерии и методики оценки эффективности систем защиты информации и действующих политик безопасности.
- Порядок организации и сопровождения аттестации объекта информатизации на соответствие требованиям защиты информации.
- Методы и средства инструментального мониторинга защищенности компьютерных систем.
- Принципы и методы разработки проектных решений по защите информации в автоматизированных системах.
- Современные методы и инструментальные средства разработки программных и программно-аппаратных средств защиты информации.
- Критерии сравнительного анализа и методы обоснованного выбора программно-аппаратных средств защиты информации.
- Принципы построения архитектуры системы защиты информации автоматизированной системы.
- Методы разработки, анализа и обоснования адекватности математических моделей процессов работы программно-аппаратных средств защиты.
- Нормативно-правовую базу и методические основы для обоснования необходимости защиты информации в автоматизированной системе.

Уметь: - Принимать участие в теоретических и экспериментальных исследованиях систем защиты информации.
- Применять математические методы в области компьютерной безопасности.
- 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 комплексного подхода к обеспечению информационной безопасности.
- 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.
- Принимать участие в разработке проектных решений по защите информации в автоматизированных системах.
- Разрабатывать программные и программно-аппаратные средства для систем защиты информации.

- Проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации.
- Принимать участие в разработке архитектуры системы защиты информации.
- Разрабатывать, анализировать и обосновывать адекватность математических моделей процессов работы средств защиты.
- Подготавливать обоснование необходимости защиты информации в автоматизированной системе.

Владеть: - Навыками проведения исследований систем защиты информации и оценки их защищенности.
- Навыками применения математических методов в области компьютерной безопасности.
- Навыками анализа исходных данных и формирования требований к системам защиты.
- Навыками разработки и конфигурирования программно-аппаратных средств защиты информации.
- Навыками реализации комплексного подхода к обеспечению информационной безопасности объекта защиты.
- Навыками оценки эффективности систем защиты информации и политик безопасности.
- Навыками анализа информационной безопасности объектов для целей аттестации.
- Навыками проведения инструментального мониторинга защищенности компьютерных систем.
- Навыками разработки проектных решений по защите информации в автоматизированных системах.
- Навыками разработки программных и программно-аппаратных средств защиты информации.
- Навыками сравнительного анализа и выбора программно-аппаратных средств защиты.
- Навыками разработки архитектуры системы защиты информации.
- Навыками разработки и анализа математических моделей процессов работы средств защиты.
- Навыками обоснования необходимости защиты информации в автоматизированных системах.

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	Этап: Подготовительный Рассматриваемые вопросы: - Вводный инструктаж на месте практики, инструктаж по охране труда и противопожарной безопасности.
2	Этап: Основной Рассматриваемые вопросы: - Выполнение производственных заданий на месте практики, сбор и обработка фактического материала. - Обработка и анализ полученного материала.
3	Этап: Заключительный Рассматриваемые вопросы: - Подготовка отчета по практике. - Защита отчета по практике.

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

№ п/п	Библиографическое описание	Место доступа
1	Методы и средства защиты информации Краковский Ю. М. Учебное пособие — 2-е изд., стер. — Санкт-Петербург : Лань, - 271 с.. — ISBN 978-5-507-52958-2. , 2025	https://reader.lanbook.com/book/463013#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 в вычислительных сетях Сафронов В. В., Кенин С. Л., Иванкин М. П., Ключников В. В. Учебно-методическое издание Воронежский государственный университет. - Воронеж: Издательский дом ВГУ, - 42 с. , 2021	https://reader.lanbook.com/book/455111#2
4	Защита информационных систем. Кибербезопасность Баланов А.Н. Учебное пособие — 3-е изд., стер. —	https://reader.lanbook.com/book/514704#2

	Санкт-Петербург: Лань, - 280 с. — ISBN 978-5-507-56255-8. , 2026	

9. Форма промежуточной аттестации: Дифференцированный зачет в 8 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 Н.А. Андриянова