

**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**

**Преддипломная 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: 01.06.2023

## 1. Общие сведения о практике.

Целями преддипломной практики являются получение практических знаний, умений и навыков, необходимых для выполнения выпускной квалификационной работы (дипломного проекта) и для успешной адаптации к рынку труда по данной специальности.

Задачами преддипломной практики являются:

- закрепление на практике теоретических знаний, полученных при изучении дисциплин базовой части;
- практическое освоение российских и международных стандартов ИБ в рамках деятельности предприятия и оценка степени их применимости для КС данного предприятия;
- приобретение навыков и опыта в проведении обследования защищенности КС и ее подсистем;
- приобретение навыков проектирования систем защиты информации для объектов информатизации;
- умение разрабатывать, апробировать и внедрять технические решения и механизмы защиты информации для конкретных КС;
- освоение технологий сопровождения программно-технических комплексов систем защиты предприятия или компании.

## 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-1** - Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;

**ОПК-2** - Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности;

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

**ОПК-4** - Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности;

**ОПК-5** - Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;

**ОПК-6** - Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

**ОПК-7** - 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-8** - Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей;

**ОПК-9** - Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации

от утечки по техническим каналам, сетей и систем передачи информации;

**ОПК-10** - Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности;

**ОПК-11** - Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации;

**ОПК-12** - Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения;

**ОПК-13** - Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности;

**ОПК-14** - Способен проектировать базы данных, администрировать системы управления базами данных в соответствии с требованиями по защите информации;

**ОПК-15** - Способен администрировать компьютерные сети и контролировать корректность их функционирования;

**ОПК-16** - Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях;

**ОПК-17** - Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма;

**ПК-1** - Способен принимать участие в теоретических и экспериментальных исследованиях систем защиты информации, проводить научно-исследовательские работы по оценке защищенности информации в компьютерных системах;

**ПК-2** - Способен применять математические методы в области компьютерной безопасности;

**ПК-3** - Способен проводить анализ исходных данных и формировать требования к компонентам и методам при проектировании подсистем и средств обеспечения информационной безопасности;

**ПК-4** - Способен участвовать в разработке подсистемы информационной безопасности компьютерной (в том числе автоматизированной) системы включая разработку программно-аппаратных

средств защиты информации, защищенных операционных систем, систем управления базами данных, компьютерных сетей, систем антивирусной защиты, средств криптографической защиты информации;

**ПК-5** - Способен участвовать в работах по проектированию и реализации комплексного подхода к обеспечению информационной безопасности объекта защиты;

**ПК-6** - Способен проводить оценку эффективности реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации;

**ПК-7** - Способен проводить анализ информационной безопасности объектов и систем, принимать участие в организации и сопровождении аттестации объекта информатизации на предмет соответствия требованиям защиты информации;

**ПК-8** - Способен проводить инструментальный мониторинг защищенности компьютерных систем;

**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-11** - Способен проводить проверки эффективности и выполнять работы по восстановлению работоспособности программных, программно-аппаратных и технических средств, подсистем защиты информации;

**ПК-12** - Способен выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности, проводить мониторинг и анализ эффективности реализации систем защиты информации и действующих политик безопасности в компьютерных системах;

**ПК-13** - Способен строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов;

**ПК-14** - Способен проводить моделирование защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации;

**ПК-15** - Способен принимать участие в разработке проектных решений по защите информации в автоматизированных системах;

**ПК-16** - Способен разрабатывать программные и программно-аппаратные средства для систем защиты информации автоматизированных систем;

**ПК-17** - Способен проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации с учетом современных и перспективных математических методов защиты информации;

**ПК-18** - Способен принимать участие в разработке архитектуры системы защиты информации автоматизированной системы;

**ПК-19** - Способен разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации;

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

**ПК-21** - Способен определять возможные угрозы безопасности информации, обрабатываемой автоматизированной системой;

**ПК-22** - Способен проводить тестирование систем защиты информации автоматизированных систем;

**ПК-23** - Способен участвовать в разработке эксплуатационной документации на системы защиты информации автоматизированных систем;

**ПК-24** - Способен разрабатывать модели угроз, формировать требования по защите информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации;

**ПК-25** - Способен разрабатывать план мероприятий по защите информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации;

**ПК-26** - Способен проводить анализ эффективности систем защиты информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации;

**ПК-27** - Способен участвовать в создании системы защиты информации процессов проектирования, создания и модернизации объектов информатизации на базе компьютерных систем;

**ПК-28** - Способен разрабатывать проекты нормативных правовых актов, руководящих и методических документов предприятия, учреждения, организации, регламентирующих деятельность по защите информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации;

**УК-1** - Способен осуществлять критический анализ проблемных

ситуаций на основе системного подхода, вырабатывать стратегию действий;

**УК-2** - Способен управлять проектом на всех этапах его жизненного цикла;

**УК-3** - Способен организовать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели;

**УК-4** - Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия;

**УК-5** - Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия;

**УК-6** - Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни;

**УК-7** - Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности;

**УК-8** - Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов;

**УК-9** - Способен использовать базовые дефектологические знания в социальной и профессиональной сферах;

**УК-10** - Способен принимать обоснованные экономические решения в различных областях жизнедеятельности;

**УК-11** - Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности.

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

**Знать:** - типовые модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах, угроз безопасности информации;

- методы, средства и нормативную базу оценки уровня безопасности компьютерных систем и сетей;

- последовательность действий по восстановлению работоспособности подсистем защиты информации в операционных системах, программно-

аппаратных средствах защиты информации, в прикладном и системном программном обеспечении;

**Уметь:** - анализировать результаты выполненных работ по восстановлению работоспособности подсистем защиты информации в операционных системах, программно-аппаратных средствах защиты информации, в прикладном и системном программном обеспечении;

- делать соответствующие выводы и строить свою деятельность в зависимости от достигнутых результатов и полученных выводов;
- Оценивает функциональные возможности аппаратных и программных средств, включая операционные системы, в составе компьютерной системы; проводит классификацию и устанавливает групповую принадлежность программного обеспечения;
- Выполняет работы по установке, настройке, администрированию и проверке работоспособности программно-аппаратные средства системного, прикладного и специального назначения в сфере профессиональной деятельности;
- Выполняет управление инцидентами безопасности при функционировании программных средств системного, прикладного и специального назначения;
- Участвует в разработке проектной и технической документации, включая технические задания, технико-экономическое обоснование и проектную документацию на разрабатываемые программные средства;
- Применяет специальные математические методы, включая криптографические, для анализа и разработки защищенных компьютерных систем.

**Владеть:** - методами и средствами мониторинга эффективности программно-аппаратных средств защиты информации в операционных системах, системах управления базами данных, компьютерных сетях;

- навыками сравнительного анализа эффективности программно-аппаратных средств защиты информации в операционных системах.

## 6. Объем практики.

Объем практики составляет 12 зачетных единиц (432 академических часов).

## 7. Содержание практики.

Обучающиеся в период прохождения практики выполняют индивидуальные задания руководителя практики.



№ п/п	Краткое содержание
1	Этап: Подготовительный этап
2	Этап: Производственный инструктаж
3	Этап: Выполнение производственных заданий
4	Этап: Анализ и обобщение фактического материала для отчета
5	Этап: Подготовка и оформление отчета по преддипломной практике
6	Этап: Проверка и защита отчета по преддипломной практике

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

№ п/п	Библиографическое описание	Место доступа
1	Поддержка принятия решений при проектировании систем защиты информации Бухтояров В.В. и др. М.: ИНФРА-М. , 2014	Internet
2	«Информационная безопасность компьютерных систем и сетей». Учебное пособие Шаньгин В.Ф. М.: ИД «Форум» , 2014	Internet
3	Организационное и техническое обеспечение ИБ. Защита конфиденциальной информации: Учебное пособие Ишейнов В.Я., Мецатунян М.В. М.: ИД «Форум» , 2014	Internet
4	Модели безопасности компьютерных систем. Управление доступом и информационными потоками: Учебное пособие для ВУЗов Девянин П.Н. М., Горячая линия – Телеком , 2011	Internet

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  
«Управление и защита информации»

М.Я. Клепцов

Согласовано:

Заведующий кафедрой УиЗИ

Председатель учебно-методической  
комиссии

Л.А. Баранов

С.В. Володин