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

Преддипломная практика

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Информационная безопасность объектов информатизации на базе компьютерных систем

Форма обучения: Очная

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 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-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 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;

ОПК-7 - Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации;

ПК-1 - 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;

ПК-2 - Способен проводить анализ информационной безопасности объектов и систем, принимать участие в организации и сопровождении аттестации объекта информатизации на предмет соответствия требованиям защиты информации;

ПК-3 - Способен принимать участие в теоретических и экспериментальных исследованиях систем защиты информации, проводить

научно-исследовательские работы по оценке защищенности информации в компьютерных системах;

ПК-4 - 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-5 - Способен участвовать в управлении информационной безопасностью компьютерной системы, разрабатывать предложения по ее совершенствованию;

ПК-6 - 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-7 - Способен разрабатывать план мероприятий по защите информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации;

ПК-8 - Способен участвовать в создании системы защиты информации процессов проектирования, создания и модернизации объектов информатизации на базе компьютерных систем;

УК-1 - Способен осмысленно подходить к решению задач, выявлять проблемы, ставить цели, вырабатывать стратегию действий;

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

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

УК-4 - Способен к продуктивной коммуникации;

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

УК-6 - Способен к рефлексии, самоанализу и самооценке;

УК-7 - Способен поддерживать должный уровень психологической, эмоциональной и физической подготовки для обеспечения полноценной социальной и профессиональной жизни;

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

УК-9 - Способен принимать обоснованные экономические решения в различных областях жизнедеятельности;

УК-10 - Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им;

УК-11 - Способен понимать роль России в современном мире, формировать национальную идентичность и патриотизм.

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

Знать: - Роль информации, информационных технологий и информационной безопасности в современном обществе.
- Программные средства системного и прикладного назначений, в том числе отечественного производства.
- Совокупность математических методов для разработки процедур решения задач профессиональной деятельности.
- Физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники.
- Нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации.
- Нормативные правовые акты и методические документы ФСБ России и ФСТЭК России в области защиты информации ограниченного доступа.
- Методы и инструментальные средства программирования для решения профессиональных задач.
- Методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей.
- Текущее состояние и тенденции развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных.
- Тенденции развития методов и средств криптографической защиты информации.
- Типовые модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах.
- Методы и последовательность действий по восстановлению работоспособности прикладного и системного программного обеспечения.
- Методы разработки и анализа безопасности компонентов программных и программно-аппаратных средств защиты информации.
- Принципы проектирования баз данных и администрирования СУБД с учетом требований по защите информации.
- Принципы администрирования компьютерных сетей и критерии корректности их функционирования.
- Методики мониторинга работоспособности и анализа эффективности средств защиты информации в компьютерных системах и сетях.

- Основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории.
- 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.
- 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.
- Основы управления информационной безопасностью компьютерной системы.
- Требования нормативных правовых актов и методических документов ФСБ России и ФСТЭК России к организации процесса защиты информации.
- Методы и средства восстановления работоспособности программных, программно-аппаратных и технических средств, подсистем защиты информации.
- Методы построения математических моделей для оценки безопасности компьютерных систем.
- Методологию моделирования защищенных автоматизированных систем с целью анализа их уязвимостей.
- 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.
- Классификацию и характеристику возможных угроз безопасности информации, обрабатываемой автоматизированной системой.
- Методики и инструментальные средства тестирования систем защиты информации автоматизированных систем.
- Структуру и содержание эксплуатационной документации на системы защиты информации.
- Методологию разработки моделей угроз и формирования требований по защите информации.
- Структуру и содержание плана мероприятий по защите информации в объектах информатизации.
- Критерии и методики проведения анализа эффективности систем защиты информации.
- Принципы организации и этапы создания системы защиты информации процессов проектирования, создания и модернизации.
- Требования к разработке проектов нормативных правовых актов, руководящих и методических документов в области защиты информации.
- Методы системного подхода для критического анализа проблемных ситуаций.
- Методологию управления проектом на всех этапах его жизненного цикла.
- Принципы организации и руководства работой команды для достижения поставленной цели.
- Современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для профессионального взаимодействия.
- Особенности межкультурного взаимодействия и разнообразие культур.
- Методы определения и реализации приоритетов собственной деятельности и способы ее совершенствования.
- Основы физической подготовленности для обеспечения полноценной профессиональной деятельности.
- Методы создания и поддержания безопасных условий жизнедеятельности, в том числе при чрезвычайных ситуациях.
- Базовые дефектологические знания в социальной и профессиональной сферах.
- Основы принятия обоснованных экономических решений в различных областях жизнедеятельности.
- Основы противодействия экстремизму, терроризму и коррупционному поведению в профессиональной деятельности.

Уметь: - Оценивать роль информации, информационных технологий и информационной безопасности в современном обществе.
- Применять программные средства системного и прикладного назначений, в том числе отечественного производства.
- Разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности на основе математических методов.
- Анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники.
- Применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации.
- Организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с требованиями ФСБ и ФСТЭК.
- Создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования.
- Применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей.
- Решать задачи профессиональной деятельности с учетом тенденций развития методов защиты информации.
- Анализировать тенденции развития методов и средств криптографической защиты информации и использовать их.
- Разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах.
- Администрировать операционные системы и выполнять работы по восстановлению работоспособности программного обеспечения.
- Разрабатывать компоненты программных и программно-аппаратных средств защиты информации и проводить анализ их безопасности.
- Проектировать базы данных и администрировать СУБД в соответствии с требованиями по защите информации.
- Администрировать компьютерные сети и контролировать корректность их функционирования.
- Проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях.
- Анализировать основные этапы и закономерности исторического развития России для формирования гражданской позиции.
- 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.
- Участвовать в управлении информационной безопасностью и разрабатывать предложения по ее совершенствованию.
- Организовывать процесс защиты информации в соответствии с требованиями ФСБ и ФСТЭК.
- Выполнять работы по восстановлению работоспособности средств и подсистем защиты информации.
- Выполнять полный объем работ по реализации частных политик информационной безопасности и мониторингу их эффективности.
- Строить математические модели для оценки безопасности компьютерных систем и анализировать их компоненты.
- Проводить моделирование защищенных автоматизированных систем с целью анализа их уязвимостей.
- 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.
- Определять возможные угрозы безопасности информации, обрабатываемой автоматизированной системой.
- Проводить тестирование систем защиты информации автоматизированных систем.
- Участвовать в разработке эксплуатационной документации на системы

защиты информации.
- Разрабатывать модели угроз и формировать требования по защите информации.
- Разрабатывать план мероприятий по защите информации в объектах информатизации.
- Проводить анализ эффективности систем защиты информации в объектах информатизации.
- Участвовать в создании системы защиты информации процессов проектирования, создания и модернизации.
- Разрабатывать проекты нормативных правовых актов и методических документов в области защиты информации.
- Осуществлять критический анализ проблемных ситуаций на основе системного подхода.
- Управлять проектом на всех этапах его жизненного цикла.
- Организовывать и руководить работой команды для достижения поставленной цели.
- Применять современные коммуникативные технологии для профессионального взаимодействия.
- Анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия.
- Определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования.
- Поддерживать должный уровень физической подготовленности для профессиональной деятельности.
- Создавать и поддерживать безопасные условия жизнедеятельности, в том числе при чрезвычайных ситуациях.
- Использовать базовые дефектологические знания в социальной и профессиональной сферах.
- Принимать обоснованные экономические решения в различных областях жизнедеятельности.
- Формировать нетерпимое отношение к проявлениям экстремизма, терроризма и коррупции.

Владеть: - Навыками оценки роли информации и информационной безопасности в современном обществе.
- Навыками применения программных средств системного и прикладного назначения.
- Навыками разработки и реализации процедур решения задач на основе математических методов.
- Навыками анализа физических процессов, лежащих в основе

функционирования микроэлектронной техники.
- Навыками применения нормативных правовых актов в области защиты информации.
- Навыками организации защиты информации ограниченного доступа в компьютерных системах и сетях.
- Навыками создания программ и применения инструментальных средств программирования.
- Навыками применения методов научных исследований при разработке систем безопасности.
- Навыками решения задач профессиональной деятельности с учетом тенденций развития методов защиты информации.
- Навыками анализа и использования методов и средств криптографической защиты информации.
- Навыками разработки политик безопасности и управления доступом в компьютерных системах.
- Навыками администрирования операционных систем и восстановления их работоспособности.
- Навыками разработки и анализа безопасности компонентов средств защиты информации.
- Навыками проектирования баз данных и администрирования СУБД с учетом требований защиты.
- Навыками администрирования компьютерных сетей и контроля их функционирования.
- Навыками мониторинга и анализа эффективности средств защиты информации.
- Навыками анализа исторических процессов для формирования гражданской позиции.
- Навыками проведения теоретических и экспериментальных исследований систем защиты информации.
- Навыками применения математических методов в области компьютерной безопасности.
- Навыками анализа исходных данных и формирования требований к системам защиты.
- Навыками разработки подсистем информационной безопасности компьютерных систем.
- Навыками реализации комплексного подхода к обеспечению информационной безопасности. (
- 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 управления информационной безопасностью и разработки предложений по ее совершенствованию.
- Навыками организации процесса защиты информации в соответствии с нормативными требованиями.
- Навыками восстановления работоспособности программно-аппаратных средств защиты информации.
- Навыками реализации частных политик информационной безопасности и мониторинга их эффективности.
- Навыками построения математических моделей для оценки безопасности компьютерных систем.
- Навыками моделирования защищенных автоматизированных систем для анализа уязвимостей.
- Навыками разработки проектных решений по защите информации.
- 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.
- Навыками определения и анализа угроз безопасности информации.
- Навыками тестирования систем защиты информации.
- Навыками разработки эксплуатационной документации на системы защиты информации.
- Навыками разработки моделей угроз и формирования требований по защите информации.
- Навыками разработки планов мероприятий по защите информации.
- Навыками анализа эффективности систем защиты информации.
- Навыками создания системы защиты информации процессов проектирования, создания и модернизации.
- Навыками разработки нормативных правовых актов и методических документов в области защиты информации.
- Навыками критического анализа проблемных ситуаций на основе системного

подхода.
- Навыками управления проектом на всех этапах его жизненного цикла.
- Навыками организации и руководства работой команды.
- Навыками применения современных коммуникативных технологий для профессионального взаимодействия.
- Навыками межкультурного взаимодействия с учетом разнообразия культур.
- Навыками определения и реализации приоритетов собственной деятельности.
- Навыками поддержания должного уровня физической подготовленности.
- Навыками создания и поддержания безопасных условий жизнедеятельности.
- Навыками использования базовых дефектологических знаний в профессиональной деятельности.
- Навыками принятия обоснованных экономических решений.
- Навыками противодействия экстремизму, терроризму и коррупционному поведению.

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	Подготовительный этап Проведение инструктажа по технике безопасности и охране труда в организации (структурном подразделении) — месте прохождения практики. Ознакомление с правилами внутреннего распорядка, противопожарной безопасностью. Получение индивидуального задания от руководителя практики. Ознакомление с программой практики, составление индивидуального плана работы. Изучение структуры организации, ее основных функций и задач в области информационной безопасности.

№ п/п	Краткое содержание
2	Основной (производственный) этап Выполнение индивидуального задания в соответствии с утвержденным планом. Сбор, обработка и анализ материалов, необходимых для выполнения выпускной квалификационной работы (дипломного проекта). Изучение и анализ применяемых в организации методов, средств и систем защиты информации. Оценка эффективности действующих политик безопасности и средств защиты. Участие в проведении обследования защищенности компьютерных систем и сетей. Участие в проектировании, настройке, тестировании и сопровождении программно-аппаратных средств защиты информации. Оформление результатов работы в виде отчетных материалов.
3	Заключительный этап Обработка и систематизация собранных материалов. Формулирование выводов и рекомендаций по результатам выполненной работы. Подготовка отчета о прохождении практики в соответствии с установленными требованиями. Оформление дневника практики. Представление отчета и защита результатов перед руководителем практики (дифференцированный зачет).

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

№ п/п	Библиографическое описание	Место доступа
1	Обработка информации в распределенных системах Фомичева С. Г. Учебное пособие — Санкт-Петербург : ГУАП, - 132 с. — ISBN 978-5-8088-1487-5. , 2020	https://reader.lanbook.com/book/165237#2
2	Комплексное обеспечение информационной безопасности на предприятии Тумбинская М. В., Петровский М. В. Учебник — 3-е изд., стер. — Санкт-Петербург: Лань, 344 с. — ISBN 978-5-507-52270-5. , 2025	https://reader.lanbook.com/book/445253#2
3	Безопасность операционных систем Потерпеев Г.Ю., Нефедов В.С., Криулин А.А. Учебное пособие — Москва : РТУ МИРЭА, - 93 с. — ISBN 978-5-7339-1393-3. , 2021	https://reader.lanbook.com/book/182416#2

4	Обработка информации в распределенных системах Фомичева С.Г. Учебное пособие — Санкт-Петербург : ГУАП, - 131 с. — ISBN 978-5-8088-1487-5. , 2020	https://reader.lanbook.com/book/165237#2
5	Управление информационной безопасностью Давыдов А. И., Елизаров Д. А. Учебное пособие Омск: ОмГУПС, - 92 с. — ISBN 978-5-949-41321-0. , 2023	https://reader.lanbook.com/book/419255#3

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 М.Я. Клепцов

Согласовано:

Заведующий кафедрой УиЗИ Л.А. Баранов

Председатель учебно-методической комиссии С.В. Володин