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

Научно-исследовательская работа

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Информационная безопасность объектов информатизации на базе компьютерных систем

Форма обучения: Очная

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 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:

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-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.

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	https://reader.lanbook.com/book/419255#3
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	https://reader.lanbook.com/book/513551#2
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	https://reader.lanbook.com/book/237770#3

4	Методы защиты информации Краковский Ю. М. Учебное пособие 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — ISBN 978-5-8114-5632-1. , 2021	https://reader.lanbook.com/book/156401#1

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» В.М. Алексеев

Согласовано:

Заведующий кафедрой УиЗИ Л.А. Баранов

Председатель учебно-методической комиссии С.В. Володин