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:

Уметь: ПК-1 Участвует в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах.

Знать: ПК-1 Изучает и анализирует отечественный и зарубежный опыт по проблемам компьютерной безопасности.

Уметь: ПК-1 Участвует в проведении экспериментально-исследовательских работ при сертификации средств защиты информации.

Уметь: ПК-2 Проводит анализ и разрабатывает под руководством квалифицированного специалиста математические модели безопасности компьютерных систем.

Уметь: ПК-2 Применяет специальные математические методы, включая криптографические, для анализа и разработки защищенных компьютерных систем.

Уметь: ПК-2 Применяет решения на основе специальных математических методов для обеспечения защищенной передачи данных в современных компьютерных сетях.

Знать: ПК-3 Изучает и обобщает опыт работы различных учреждении?, организации? и предприятии? в области повышения эффективности защиты информации.

Уметь: ПК-3 Формирует требования по защите информации, включая использование математического аппарата для решения прикладных задач.

Уметь: ПК-3 Составляет планы этапов проведения научно-исследовательских и опытно- конструкторских работ.

Уметь: ПК-3 Разрабатывает и анализирует структурные и функциональные схемы защищенных компьютерных систем в сфере

профессиональной деятельности.

Уметь: ПК-4 Осуществляет рациональный выбор технологии, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасности, создаваемых защищенных компьютерных систем в сфере профессиональной деятельности.

Уметь: ПК- 4 Проектирует и разрабатывает компоненты защищенных автоматизированных систем в сфере профессиональной деятельности.

Уметь: ПК-5 Принимает участие в формировании политики информационной безопасности, ее реализации и контроле выполнения.

Уметь: ПК-5 Формирует, организует и поддерживает комплекс мер по обеспечению информационной безопасности.

Уметь: ПК-6 Подбирает методики и инструментарий, определяет критерии и осуществляет проверку эффективности 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.

Уметь: ПК-7 Проводит анализ безопасности компьютерных систем, в том числе с использованием методов моделирования, на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности.

Уметь: ПК-7 Участвует в проведении экспериментально-исследовательских работ при аттестации объектов с учетом требовании? к уровню защищенности компьютерной системы.

Уметь: ПК-7 Вырабатывает рекомендации в связи с проведенным анализом безопасности, в том числе для принятия решения о повторной аттестации компьютерной системы (в том числе автоматизированных систем), предложения по устранению выявленных уязвимостей.

Уметь: ПК-8 Анализирует защищенность компьютерных систем с использованием сканеров безопасности.

Уметь: ПК-8 Анализирует защищенность сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем.

Уметь: ПК-9 Разрабатывает и организует выполнение мероприятий в соответствии с положениями политики информационной безопасности и защиты информации ограниченного доступа.

Уметь: ПК-9 Разрабатывает предложения по совершенствованию системы управления информационной безопасностью компьютерной системы.

Уметь: ПК-9 Разрабатывать проекты нормативных правовых актов и методические материалы, регламентирующие работу по обеспечению информационной безопасности компьютерных систем.

Уметь: ПК-10 Проверяет уровень квалификации, распределяет полномочия и контролирует выполнение инструкций в отношении персонала обслуживающего технические, программные и программно-аппаратные средства защиты информации.

Уметь: ПК-10 Анализирует компьютерные системы в сфере профессиональной деятельности с целью выявления условий, способствующих совершению правонарушений в отношении сведений ограниченного доступа.

Уметь: ПК-11 Обосновывает критерии и рассчитывает показатели эффективности защиты обрабатываемой информации.

Уметь: ПК-11 Составляет методики тестирования, подбирает инструментарии? и осуществляет проверку эффективности функционирования программных, программно-аппаратных и технических средств, подсистем защиты информации.

Уметь: ПК-11 Выполняет работы по восстановлению работоспособности программных, программно-аппаратных и технических средств, подсистем защиты информации.

Уметь: ПК-12 Выполняет работы, связанные с реализацией частных политик информационной безопасности автоматизированной системы.

Уметь: ПК-12 Проводит мониторинг и аудит безопасности компьютерной системы в сфере профессиональной деятельности.

Уметь: ПК-12 Формирует основные показатели и критерии эффективности, оценивает эффективность компьютерной системы и ее средств защиты в области профессиональной деятельности.

Уметь: ПК-13 Строит математические модели для оценки безопасности компьютерных систем.

Уметь: ПК-13 Анализирует компоненты системы безопасности с использованием современных математических методов.

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
2	Этап: Рациональные приемы поиска научно - технической информации
3	Этап: Исследования в области защиты информации, связанные с темой дипломной работы

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

№ п/п	Библиографическое описание	Место доступа
1	Функциональная надежность информационных систем Шубинский И. Б. Журнал Надежность. , 2012	НТБ МИИТ
2	Прикладные информационные системы управления надежностью, безопасностью, рисками и ресурсами на железнодорожном транспорте. Замышляев А.М. Надежность. , 2013	НТБ МИИТ
3	Структурная надежность информационных систем Шубинский И. Б. Журнал Надежность.	НТБ МИИТ
4	ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования Стандартинформ. , 2013	НТБ МИИТ
5	ГОСТ Р 53113.2-2009 Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов Стандартинформ. , 2012	НТБ МИИТ
6	ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель Стандартинформ. , 2012	НТБ МИИТ
1	Информатизация на железнодорожном транспорте. История и современность В.С. Наговицын, Э.С. Поддавашкин, И.В. Харланович, Ю.С. Хандкаров; Под ред. И.В. Харлановича Однотомное издание ВЕЧЕ , 2005	НТБ (БР.); НТБ (фб.)
2	Сети передачи данных информационных систем железнодорожного траспорта на базе коммутаторов и маршрутизаторов CISCO Васин В.В. Маршрут. , 2005	НТБ МИИТ
3	ГОСТ Р ИСО/МЭК ТО 19791-2008 Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем Стандартинформ. , 2013	НТБ МИИТ

4	Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта В.В. Яковлев, А.А. Корниенко Однотомное издание УМК МПС России , 2002	НТБ (уч.4); НТБ (фб.); НТБ (чз.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»	Алексеев Виктор Михайлович

Лист согласования

Заведующий кафедрой УиЗИ	Л.А. Баранов
Председатель учебно-методической комиссии	С.В. Володин