

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

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 РУТ (МИИТ)
ID подписи: 2053
Подписал: заведующий кафедрой Баранов Леонид
Аврамович
Дата: 01.06.2024

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 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:

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-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.

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

Знать: - программные и программно-аппаратные средства для систем защиты информации автоматизированных систем
- математические методы в области компьютерной безопасности
- нормативно-правовые документы в области информационной и компьютерной безопасности

Уметь: - разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации
- участвовать в работах по проектированию и реализации комплексного подхода к обеспечению информационной безопасности объекта защиты
- проводить инструментальный мониторинг защищенности компьютерных систем

Владеть: - навыками сравнительного анализа и осуществлять обоснованный выбор программно-аппаратных средств защиты информации с учетом современных и перспективных математических методов защит

ыинформации

- навыками анализа исходных данных и формировать требования к компонентам и методам при проектировании подсистем и средств обеспечения информационной безопасности
- навыками оценивания эффективности реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные систем, системы управления базами данных, компьютерных сети, системы антивирусной защиты, средства криптографической защиты информации

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 | Средства защиты информации на железнодорожном транспорте (Криптографические методы и средства) А.А. Корниенко, М.А. Еремеев, С.Е. Ададунов; Ред. А.А. | НТБ (ЭЭ); НТБ (уч.3); НТБ (фб.); НТБ (чз.2) |

| | | |
|---|--|---|
| | Корниенко; Под Ред. А.А. Корниенко Однотомное издание Маршрут , 2006 | |
| 2 | Основы информационной безопасности и защиты сведений, составляющих, государственную тайну В.Н. Кухарев Книга Юридический институт МИИТа , 2005 | ИТБ УЛУПС (Абонемент ЮИ) |
| 1 | Модели безопасности компьютерных систем П.Н. Девянин Однотомное издание Академия , 2005 | ИТБ (фб.) |
| 2 | Информационная безопасность и защита информации В.П. Мельников, С.А. Клейменов, А.М. Петраков Книга Издательский центр "Академия" , 2012 | ИТБ УЛУПС (Абонемент ЮИ); ИТБ УЛУПС (ЧЗ1 ЮИ) |

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
«Управление и защита информации»

В.М. Алексеев

А.В. Ваганов

Согласовано:

Заведующий кафедрой УиЗИ

Л.А. Баранов

Председатель учебно-методической
комиссии

С.В. Володин