**Примерные оценочные средства применяемые при аттестации
по «Эксплуатационной практике»**

При проведении аттестации обучающемуся требуется предоставить и защитить отчет с выполненным заданием, выданным в первый день практики. Отчет состоит из:

1. Титульный лист (см. приложение 1)
2. Рабочий график (план) прохождения практики (см. приложение 3)
3. Тело отчета (требования по оформлению и структуре отчета см. приложение 2)

Отсутствие отчета или несоответствие содержанию и стандартам оформления являются основанием для неудовлетворительной оценки результатов прохождения практики.

**Приложение 1**

**МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ**

**федеральное государственное автономное образовательное**

**учреждение высшего образования**

**«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»**

**(РУТ(МИИТ)**

Кафедра «Вычислительные системы, сети и информационная безопасность»

**Отчет По**

**Эксплуатационной практике**

*Направление: 09*.03.01*Информатика и вычислительная техника*

*Профиль:**Вычислительные системы и сети*

Место прохождения практики

Студента (ФИО) группы

Руководитель практики

от кафедры \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(должность, ФИО)

**ПРИЛОЖЕНИЕ 2**

**Требования к оформлению отчета по практике**

По результатам эксплуатационной практики студент составляет индивидуальный письменный отчет по практике. Отчет должен содержать конкретные сведения о работе, проделанной в период практики, и отражать результаты выполнения заданий, предусмотренных программой практики.

 Рекомендуется следующий порядок размещения материалов в отчете:

1. ТИТУЛЬНЫЙ ЛИСТ. Образец титульного листа приведен
в приложении 1.
2. ОГЛАВЛЕНИЕ (автособираемое). Представляет собой перечень приведенных в отчете разделов и тем с указанием страниц.
3. ВВЕДЕНИЕ. Здесь формулируются цель и задачи практики
4. ОСНОВНОЙ РАЗДЕЛ. обзор проблемных вопросов, вынесенных к рассмотрению в рамках практики
5. ВЫВОДЫ. Студент оценивает новые знания, умения и практический опыт, приобретенный в процессе прохождения практики, делает свои выводы по результатам анализа собранной в процессе прохождения практики информации.
6. Список использованных источников. Список литературы должен содержать перечень источников, использованных при выполнении отчета.
7. Приложения. Приложения должны начинаться с нового листа и иметь сквозную нумерацию арабскими цифрами, с указанием в правом верхнем углу слова «Приложение».

Подготовку к написанию отчёта о практике студент осуществляет в течение всего периода её прохождения. Объём отчёта о практике не менее 25 страниц компьютерного набора.

Отчет по практике состоит из следующих разделов:

1. Титульный лист (Приложение 1)

Введение (кратко описывается цель практики, её связь с избранной специальностью, основные результаты).

Раздел 1. Аппаратное и программное обеспечение кафедры

• Аппаратное обеспечение и периферийные устройства и другая оргтехника.

• Системное программное обеспечение кафедры, названия и версии операционных систем, установленных на ПК и серверах, перечень и особенности использования системных, администраторских утилит

• Перечень прикладного программного обеспечения, используемого на кафедре и перечень задач, решаемых с их помощью.

Раздел 2. Индивидуальное задание

• Описание индивидуального задания;

• Выбор и обоснованность инструментария для выполнения задания.

• Выполнение задания

Заключение завершает отчёт. В разделе подводятся итоги практики, приводится анализ работы, выполненной во время практики и информации, полученной в ходе её проведения.

Библиографический список содержит библиографические сведения всех источников информации.

Правила оформления отчета.

Отчет должен быть написан на русском языке. Текст следует печатать на одной стороне листа белой бумаги формата А4. Цвет шрифта - черный.

1. Основные правила.

1.1 Отчет оформляется в текстовом редакторе и предоставляется на проверку в формате .doc (MS Office 2003 и выше).

1.2 Ориентация страниц: книжная.

1.3 Поля документа:

• верхнее –2 см (20 мм);

• нижнее –2 см (20 мм);

• левое – 3,5 см (35 мм);

• правое – 1 см (10 мм).

1.4 Соблюдение полей обязательно при размещении любых иллюстраций, таблиц, формул и их подписей.

1.5 Каждый новый раздел начинается с новой страницы.

1.6 Разрывы текста внутри раздела не допускаются (не должно быть «лишних» пробелов и пустых абзацев, за исключением оговоренных ситуаций).

1.7 Горизонтальное выравнивание:

• основной текст выравнивается по ширине;

• все заголовки и подписи к рисункам выравниваются по центру;

• иллюстрации, таблицы и формулы выравнивают по центру страницы.

1.8 После заголовка раздела или подраздела должен идти текст. Текст раздела не может начинаться с формулы, рисунка, таблицы и т.д.

1.9 Фамилии и собственные имена, названия учреждений в тексте магистерской диссертации приводят на языке оригинала.

1.10 Сокращения русский слов и словосочетаний следует использовать по ГОСТ Р 7.0.12-2011. Из сокращенных названий учреждений и предприятий следует употреблять только общеизвестные. Малоизвестные сокращения необходимо расшифровывать при первом упоминании.

1.11 Сокращения слов, кроме разрешенных ГОСТ 2.316-2008 ЕСКД и общепринятых (например, ТУ, ТЗ, ОЗУ, ПЗУ, АЛУ и др.) не допускаются. При необходимости сокращенного обозначения сигналов или шин следует привести описок сокращений.

1.12 В тексте следует применять стандартизированные единицы физических величин, их наименования и обозначения в соответствии с ГОСТ 8.417.

2. Параметры шрифта.

2.1 Используемый шрифт – Times New Roman.

2.2 Размеры шрифта:

• для основного текста – 14;

• заголовки первого уровня – 16 полужирный (bold);

• заголовки второго и ниже уровней – 14 полужирный (bold);

• подписи к рисункам и таблицам – 10;

• номера страниц - 12.

2.3 Отступ первой строки абзаца – 1,25 см.

2.4 Интервал между строками – 1,5.

2.5 Интервалы перед и после абзацев – 0 пт.

2.6 Тип и размер шрифта внутри рисунков может быть любым. Для листингов рекомендуется использовать шрифт Courier New, размер 10.

2.7 Размер шрифта в таблицах и междустрочный интервал можно уменьшать.

Отсутствие отчета или несоответствие содержанию и стандартам оформления являются основанием для неудовлетворительной оценки результатов прохождения практики.

Москва 20 г.

**Приложение 3**

**Совместный график (план) прохождения практики**

Фамилия, имя, отчество обучающегося \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Специальность/направление подготовки: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Специализация/профиль/направленность (бакалавриат): \_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Учебная группа \_\_\_\_\_\_\_\_\_ Курс \_\_\_

Вид практики \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Срок прохождения практики: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Объект практики:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Вид рабочей деятельности обучающегося** | **Сроки** | **Освоенные компетенции в соответствии с рабочей программой практики** |
| 1 | Оформление на работу, инструктаж по технике безопасности  |  | ОПК-7 Способность участвовать в настройке и наладке программно-аппаратных комплексов;ОПК-8 Способность разрабатывать алгоритмы и программы, пригодные для практического применения;  |
| 2 | Знакомство с предприятием, его структурой и видами деятельности.  |  | ОПК-9 Способность осваивать методики использования программных средств для решения практических задач; |
| 3 | Изучение технологического процесса работы предприятия, анализ основных показателей работы предприятия |  | ПК-5 Способность администрировать процесс управления безопасностью сетевых устройств, программного обеспечения, средств обеспечения безопасности удаленного доступа; |
| 4 | Сбор материала, необходимого для последующего выполнения выпускной квалификационной работы в соответствии с индивидуальным заданием, полученным от руководителя |  | ПК-6 Способность выполнять работы и управлять работами по разработке архитектур и прототипов информационных систем; |
| 5 | Оформление и защита отчета |  | ПК-7 Способность выполнять работы и управлять работами по созданию, модификации и сопровождению информационных систем, автоматизирующих задачи организационного управления и бизнес-процессы |

|  |  |
| --- | --- |
| Руководитель практики от университета\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (подпись) (Ф.И.О.)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (должность) | Руководитель практики от производства\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (подпись) (Ф.И.О.)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (должность) |

Вопросы для устного опроса на защите отчета

ОПК-7

1. Концепции безопасности. Преимущества применения системы защиты. Компоненты защиты.
2. Защита административных интерфейсов. Усиление парольной защиты.
3. Системы парольной аутентификации. Локальное хранение и сравнение.
4. Этапы формирования системы безопасности и оценка ее состояния.
5. Защита административных интерфейсов с помощью аутентификации и усиление парольной защиты по линиям vty.
6. Системы парольной аутентификации. Централизованное хранение.
7. Виды политик защиты.
8. Многоуровневая система привилегий доступа.
9. Системы парольной аутентификации. CHAP и MS-CHAP.
10. Недостатки системы защиты.

ОПК-8

1. Защита связи между маршрутизаторами. Аутентификация протоколов маршрутизации.
2. Системы парольной аутентификации. Kerberos. Управление ключами.
3. Вредоносные программы.
4. Защита конфигурационных файлов маршрутизатора.
5. Системы парольной аутентификации. Этапы аутентификации Kerberos.
6. Типы атак. Разведка и методы противодействия.
7. Управление обновлениями маршрутной информации.
8. Системы с одноразовыми паролями.
9. Типы атак. Несанкционированный доступ и методы противодействия.
10. Настройка локальной аутентификации ААА. Список методов аутентификации.

ОПК-9

1. Аутентификация по сертификатам.
2. Типы атак. Блокирование сервиса и методы противодействия.
3. Настройка удаленной аутентификации ААА.
4. Блочное шифрование.
5. Типы атак. Подмена данных сервиса и методы противодействия.
6. Настройка авторизации AAA.
7. Требования к алгоритму шифрования.
8. Защита административного доступа к сетевым устройствам. Защита на уровне физического доступа к устройствам. Защита на уровне административного интерфейса.
9. Настройка аудита ААА.

ПК-5

1. Блочный шифр на основе сетей Фейстеля.
2. Технология защиты ААА. Аутентификация и режимы доступа. Методы аутентификации, авторизации и аудита.
3. Работа и настройка Reflexive IP ACL.
4. Алгоритм DES.
5. Серверы защиты ААА. TACACS+.
6. Работа и настройка Dynamic ACL.
7. Режимы работы алгоритма DES.
8. Серверы защиты ААА. RADIUS.
9. Работа и настройка Time-Based ACL.
10. Тройной DES с двумя ключами.
11. Классификация вирусов.
12. Задачи и принципы работы CBAC.
13. Преобразования алгоритма Rijndael
14. Особенности алгоритма вирусов.
15. Работа CBAC с TCP и UDP.
16. Алгоритм ГОСТ 28147.
17. Модели обороны.
18. Настройка CBAC.

ПК-6

1. Алгоритм шифрования RSA.
2. Структура защищенной сети.
3. Этапы настройки IPSec VPN.
4. Электронная цифровая подпись.
5. Разделение сети на зоны. Элементы зонной структуры.
6. Настройка списка доступа, совместимого с конфигурацией IPSec.
7. Алгоритм DSA.
8. Контроль сервисов TCP/IP.
9. Настройка политики ISAKMP.
10. Шифрование сетевого уровня.
11. Задачи шифрования.
12. Настройка политики ISAKMP. Предустановленные ключи.
13. Принципы работы средств шифрования и применение шифрования.

ПК-7

1. Защита от блокирования сервисов. Защита от синхронных и асинхронных атак.
2. Определение набора преобразований IPSec.
3. Обзор технологии виртуальных частных сетей. Топологии сетей VPN.
4. Создание криптографической карты. Конфигурационные параметры. Правила формирования. Конфигурирование.
5. Протоколы для поддержки VPN.
6. Протоколы IPSec.
7. Работа IPSec. Начало процесса IPSec Работа IPSec. Первая фаза IKE. Энергичный режим.
8. Работа IPSec. Вторая фаза IKE. Передача данных. Завершение работы туннеля IPSec.