Федеральное государственное образовательное бюджетное

учреждение высшего образования

**«Финансовый университет при Правительстве Российской Федерации»**

**(Финансовый университет)**

**Липецкий филиал Финуниверситета**

УТВЕРЖДАЮ

Заместитель директора

по учебно-методической работе

Липецкого филиала Финуниверситета

\_\_\_\_\_\_\_\_\_\_ О.Н. Левчегов

«*24*» *сентября* 20*24* г.

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ**

**производственной практикИ (по ПРОФИЛЮ СПЕЦИАЛЬНОСТИ) ПП.02 в составе**

**пм.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты**

по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

*Рекомендовано Ученым советом Липецкого филиала,*

*протокол № 19 от 24 сентября 2024 года*

Липецк - 2024

Фонд оценочных средств разработан на основе федерального государственного образовательного стандарта среднего профессионального образования (далее – ФГОС СПО) по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем».

Разработчики:

Черпаков Игорь Владимирович, к.ф.-м.н., доцент кафедры Учет и информационные технологии в бизнесе Липецкого филиала Финуниверситета.

Фонд оценочных средств рассмотрен и рекомендован к утверждению   
на заседании кафедры Учет и информационные технологии в бизнесе Липецкого филиала Финуниверситета.

Протокол от 27.08.2024 г. №1

Заведующий кафедрой

Учет и информационные технологии в бизнесе \_\_\_\_\_\_\_\_\_\_ Н.С. Морозова

1. **Общие положения**

Фонд оценочных средств (далее ФОС) предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу производственной практики (по профилю специальности) по профессиональному модулю: ПМ.02. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты.

ФОС включают контрольные материалы для проведения текущего контроля и итоговой аттестации в форме зачета.

ФОС разработаны на основании положений:

* ФГОС по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем;
* программы профессионального модуля ПМ.02. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты.

**2. Результаты освоения производственной практики (по профилю специальности), подлежащие проверке**

|  |  |
| --- | --- |
| **Иметь практический опыт** | О4 – применения программно-аппаратных средств обеспечения информационной безопасности;  О5 – диагностики, устранение отказов и восстановления работоспособности программно- аппаратных средств обеспечения информационной безопасности;  О6 – мониторинга эффективности программно-аппаратных средств обеспечения информационной безопасности;  О7 – обеспечение учета, обработки, хранения и передачи конфиденциальной информации;  О8 – решение частных технических задач, возникающих при аттестации объектов, помещений, программ, алгоритмов;  О9 – применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами. |
| **Уметь** | У20 – применять программно-аппаратные средства обеспечения информационной безопасности;  У21 – диагностировать, устранять отказы и обеспечивать работоспособность программно- аппаратных средств обеспечения информационной безопасности;  У22 – оценивать эффективность применяемых программно-аппаратных средств обеспечения информационной безопасности;  У23 – участвовать в обеспечение учета, обработки, хранения и передачи конфиденциальной информации;  У24 – решать частые технические задачи, возникающие при аттестации объектов, помещений, программ, алгоритмов;  У25 – использовать типовые криптографические средства и методы защиты информации, в том числе и электронную цифровую подпись;  У26 – применять нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности программно-аппаратными средствами. |
| **Знать** | З33 – методы и формы применения программно-аппаратных средств обеспечения  информационной безопасности;  З34 – особенности применения программно-аппаратных средств обеспечения информационной безопасности в операционных системах, компьютерных сетях, базах данных;  З35 – типовые модели управления доступом;  З36 – типовые средства, методы и протоколы идентификации, аутентификации и авторизации;  З37 – типовые средства и методы ведения аудита и обнаружение вторжений;  З38 – типовые средства и методы обеспечения информационной безопасности в локальных и глобальных вычислительных сетях;  З39 – основные понятия криптографии и типовые криптографические методы защиты информации. |

**3. Содержание практики**

Во время прохождения производственной практики (по профилю специальности) обучающийся должен:

* прослушать инструктаж по технике безопасности в ходе прохождения практики;
* ознакомиться с целями, задачами производственной практики (по профилю специальности);

Обучающиеся перед прохождением производственной практики (по профилю специальности) обеспечиваются программой прохождения практики и индивидуальным заданием руководителя практики от организации. В процессе прохождения практики обучающиеся должны использовать компьютерную технику, а именно: во время выполнения работы и отчета по производственной практике используют ПК. Самостоятельная работа обучающихся подразумевает работу под руководством руководителя практики и/или преподавателей, осуществляющих руководство производственной практикой. Проводя собеседование, руководитель практики/преподаватели обсуждают с обучающимися план будущей практики, формируют вопросы, которые необходимо раскрыть при составлении отчета о практике, объясняют порядок заполнения дневника прохождения практики и подписывают его, дают рекомендации по изучению необходимого нормативного материала, применению соответствующей литературы. В дневнике прохождения производственной практики (по профилю специальности) отражается краткое содержание работ, выполняемых обучающимся. Записи должны вносится обучающимися ежедневно, отражая данные о проделанной работе и заверяется подписью и печатью руководителя по месту прохождения практики. В ходе прохождения практики обучающемуся следует обратиться к рекомендованным руководителем практики нормативно-правовым документам, специальной литературе, другим материалам, опубликованным в печати. В соответствии с описанными задачами обучающийся собирает и обрабатывает информацию для написания отчета. По окончании практики обучающийся в установленные сроки сдает руководителю практики от Липецкого филиала отчет о практике. Отчет по практике содержит титульный лист, содержание (план), текстовую часть, список литературы, приложения, дневник, характеристику.

Необходимым компонентом производственной практики (по профилю специальности) является выполнение индивидуального задания. Индивидуальное задание на практику направлено на углубление и расширение полученных студентами знаний в области информационной безопасности, которое является одним из необходимых условий дальнейшего освоения дисциплин профессионального цикла.

Рекомендуемые темы индивидуальных заданий:

* Анализ объектов информатизации на предприятии, учреждении, организации.
* Анализ ресурсов обеспечения защиты информации.
* Анализ видов ущерба, наносимого информации.
* Анализ степени наносимого ущерба информации.
* Оценка эффективности защиты информации.
* Изучение технических средств защиты информации.
* Анализ видов информации, защищаемой техническими средствами.
* Изучение основных этапов проектирования системы защиты информации техническими средствами.
* Изучение системы технических средств охраны (ТСО).
* Изучение принципов организации и этапов разработки комплексной системы защиты информации (КСЗИ).

Тема индивидуального задания каждого конкретного студента, как правило, совпадает с профилем и спецификой работы предприятия – места прохождения практики. Результаты выполнения индивидуального задания оформляются в виде реферата, входящего в состав отчета по практике в качестве его основного раздела.

**4. Форма отчетности**

Обязательными отчетными документами по практике являются:

* отчет по практике;
* дневник прохождения практики;

Отчет по производственной практике оформляется в виде текстового документа с соблюдением требований действующих ГОСТов. Формы титульного листа отчета по прозводственной практике и дневника ее прохождения представлены в Приложениях А и Б соответственно.

**5. Информационные технологии, используемые при проведении практики**

1. Операционная система Windows Professional 7.
2. Пакет программ Open Office.
3. Интернет-браузеры Mozilla Firefox, Google Chrome, Opera (последние версии).
4. Программа для просмотра и чтения файлов формата. djvu Djvu reader (последняя версия).
5. Программа для просмотра и чтения файлов формата .pdf Acrobat Reader (последняя версия).
6. Пакет программ семейства MS Office.
7. Поисково-справочная система Google. – Режим доступа: https://www.google.ru/
8. Поисково-справочная система Яндекс. – Режим доступа: https://www.yandex.ru/

**6. Критерии и шкалы оценивания**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Вид контроля | Форма аттестации | Оценочные средства | Критерии оценивания | Шкала оценивания |
| Промежуточная аттестация | Зачет | Отчет о прохождении производственной практики (по профилю специальности) | Отчет о прохождении практики оформлен не надлежащим образом или при его защите студент демонстрирует непонимание задач практики, дает правильные ответы менее чем на 25 % заданных контрольных вопросов. | Не зачтено |
| Отчет о прохождении практики, в целом оформлен надлежащим образом, при его защите студент демонстрирует общее понимание задач практики, дает правильные ответы на 25 – 50 % заданных контрольных вопросов. | 3 (удовлетворительно) |
| Отчет о прохождении практики оформлен надлежащим образом, при его защите студент демонстрирует полное понимание задач практики, дает правильные ответы на 50 – 75 % заданных контрольных вопросов | 4 (хорошо) |
| Отчет о прохождении практики оформлен надлежащим образом, при его защите студент демонстрирует полное понимание задач практики, дает правильные ответы на 75 – 100 % заданных контрольных вопросов. | 5 (отлично) |

**Оценочные материалы**

1. Выберите один верный ответ.

*Сетевой администратор реализует политику, требующую надежных и сложных паролей. Укажите цель защиты данных поддерживающую данную политику.*

А) достоверной

Б) конфиденциальной

В) документированной

2. Выберите один верный ответ.

*Формы защиты интеллектуальной собственности -*

А) авторское, патентное право и коммерческая тайна

Б) интеллектуальное право и смежные права

В) коммерческая и государственная тайна

3. Выберите один верный ответ.

*По принадлежности информационные ресурсы подразделяются на*

А) государственные, коммерческие и личные

Б) государственные, не государственные и информацию о гражданах

В) информацию юридических и физических лиц

4. Выберите один верный ответ.

*К конфиденциальной информации относятся документы, содержащие*

А) государственную тайну

Б) законодательные акты

В) "ноу-хау"

5. Выберите один верный ответ.

*Запрещено относить к информации ограниченного доступа*

А) информацию о чрезвычайных ситуациях

Б) информацию о деятельности органов государственной власти

В) документы открытых архивов и библиотек

6. Выберите один верный ответ.

*Основными источниками угроз информационной безопасности являются все указанное в списке:*

А) хищение жестких дисков, подключение к сети, инсайдерство

Б) перехват данных, хищение данных, изменение архитектуры системы

В) хищение данных, подкуп системных администраторов, нарушение регламента работы

7. Выберите один верный ответ.

*Какие угрозы безопасности информации являются преднамеренными:*

А) ошибки персонала

Б) открытие электронного письма, содержащего вирус

В) не авторизованный доступ

8. Выберите один верный ответ.

*Какие методы обеспечения информационной безопасности Российской Федерации направлены на создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи?*

А) правовые

Б) организационно-технические

В) экономические

9. Выберите один верный ответ.

*Что использует системы защиты информации Secret Disk для хранения паролей?*

А) накопители на магнитных дисках

Б) оперативную память компьютера

В) электронные ключи

10. Выберите один верный ответ.

*С какой целью используется теория информации при рассмотрении каналов передачи информационных потоков?*

А) для повышения эффективности работы каналов связи

Б) для анализа качества передаваемой информации

В) для вычисления количества информации в потоке и пропускной способности канала

11. Выберите один верный ответ.

*Какие преобразования шифра выполняются при операции рассеивания?*

А) сжатие шифра

Б) передача текста небольшими частями

В) изменение любого знака открытого текста или ключа

12. Выберите один верный ответ.

*Как называется режим использования блочного шифра, в котором каждый блок исходных данных шифруется независимо от остальных блоков с применением одного и того же ключа шифрования?*

А) режим простой поблочной замены

Б) режим сцепления блоков шифра

В) режим формирования электронной цифровой подписи

Г) режим создания хеш-кода

13. Выберите один верный ответ.

*Как называется режим использования блочного шифра, в котором перед шифрованием каждый блок открытого текста складывается по модулю 2 с результатом шифрования предыдущего блока?*

А) режим простой поблочной замены

Б) режим сцепления блоков шифра

В) режим формирования электронной цифровой подписи

14. Выберите один верный ответ.

*Алгоритм DES является*

А) алгоритмом вычисления функции хеширования

Б) алгоритмом формирования электронной цифровой подписи

В) блочным алгоритмом асимметричного шифрования

Г) блочным алгоритмом симметричного шифрования

15. Выберите один верный ответ.

*Как называется совокупность заранее оговоренных способов преобразования исходного секретного сообщения с целью его защиты?*

А) алгоритм

Б) ключ

В) протокол

Г) шифр.

**Критерии оценки**

|  |  |  |
| --- | --- | --- |
| **Объем выполнения, %** | **Оценка** | **Критерии оценки** |
| от 86 до 100 | Зачет | *-* теоретическое содержание предмета освоено полностью, сформированы необходимые практические навыки и умения, выполнены все задания. |
| от 70 до 85 | теоретическое содержание предмета освоено полностью, сформированы необходимые практические навыки и умения не в полном объеме, выполнены все задания, при выполнении которых были обнаружены ошибки и недочеты. |
| от 50 до 69 | теоретическое содержание предмета освоено частично, но пробелы не носят существенного характера, сформированы в основном необходимые практические навыки и умения, выполнено большинство заданий, при выполнении которых были обнаружены ошибки и недочеты. |
| от 0 до 49 | «Незачет» | теоретическое содержание предмета не освоено, не сформированы необходимые практические навыки и умения, выполненные учебные задания содержат ошибки и недочеты. |

**Ключ (правильные ответы)**

1. Ответ: в

2. Ответ: а

3. Ответ: б

4. Ответ: а

5. Ответ: а

6. Ответ: б

7. Ответ: в

8. Ответ: б

9. Ответ: в

10. Ответ: в

11. Ответ: в

12 Ответ: а

13. Ответ: б

14. Ответ: г

15. Ответ: г

**Список использованной литературы**

1. Федеральный закон «О техническом регулировании». **–** URL: https://base.garant.ru/12129354/.
2. Стандарты и регламенты//РОССТАНДАРТ. Федеральное агентство по техническому регулированию и метрологии: официальный сайт. - URL: https://www.rst.gov.ru/portal/gost//home/standarts.
3. Правила по проведению сертификации в Российской Федерации. **–** URL: http://www.consultant.ru/document/cons\_doc\_LAW\_27857/d2734ce73fb57447db7ca97c3e9 550b7b847e56a/.
4. Техэксперт. Электронный фонд правовой и нормативно-технической документации/АО «Кодекс»: Профессиональные справочные системы: официальный сайт. **–**URL: http://docs.cntd.ru**/.**
5. ГОСТ 8.417-2002. Государственная система обеспечения единства измерений (ГСИ). Единицы величин (с поправками). **–** URL: http://docs.cntd.ru/document/1200031406.
6. ГОСТ Р 1.0-2004. Стандартизация в Российской Федерации. Основные положения. **–** http://docs.cntd.ru/document/1200038794.
7. ГОСТ Р 8.563-2009 Государственная система обеспечения единства измерений (ГСИ). Методики (методы) измерений. **–**URL: http://docs.cntd.ru/document/1200077909.
8. ГОСТ Р 8.000-2015 Государственная система обеспечения единства измерений (ГСИ). Основные положения. **–**URL: http://docs.cntd.ru/document/1200124116.
9. ОСТ 45.150-99 Отраслевая система обеспечения единства измерений. Методики выполнения измерений. Порядок разработки и аттестации. **–** URL: http://docs.cntd.ru/document/1200036493.
10. ГОСТ Р 40.002-2000 Система сертификации ГОСТ Р. Регистр систем качества. Основные положения. –URL: http://docs.cntd.ru/document/1200006218.
11. ГОСТ Р 1.0-92 Государственная система стандартизации РФ. Основные положения. – URL: http://docs.cntd.ru/document/5200306.

**Электронные издания:**

1. Нефедов, В.И. Теория электросвязи: учебник для студ. учрежд. СПО /В.И.Нефедов, А.С.Сигов. - Москва: Юрайт, 2020.
2. Ситников, А. В. Электротехнические основы источников питания: учебник для студ. учрежд. СПО/ А.В. Ситников, И.А. Ситников. - Москва: КУРС: ИНФРА-М, 2020.
3. Хрусталева, З.А. Метрология, стандартизация и сертификация. Практикум: учебное пособие для студ. учрежд. СПО/ З.А.Хрусталева. - Москва: КноРус, 2020.
4. Шишмарёв, В.Ю. Метрология, стандартизация, сертификация, техническое регулирование и документоведение: учебник для студ. учрежд. СПО/В.Ю.Шишмарев. – Москва: КУРС: ИНФРА-М, 2020.
5. Электрорадиоизмерения: учебник для студ. учрежд. СПО /В.И.Нефедов, А.С.Сигов, В.К.Битюков, Е.В.Самохина; под ред. А.С.Сигова. - Москва: Форум: Инфра-М, 2020.

**Электронные ресурсы:**

1. 1. Федеральное агентство связи (Россвязь): официальный сайт. Документы. **–** URL: https://rossvyaz.gov.ru/dokumenty.
2. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации: официальный сайт. **–** URL: http://www.minsvyaz.ru/.
3. Федеральная служба по техническому и экспортному контролю (ФСТЭК России): официальный сайт. – URL: www.fstec.ru.
4. Информационно- коммуникационные технологии в образовании: федеральный портал. – URL: htpp\\:www.ict.edu.ru.
5. Convertworld.com. Перевод единиц измерения онлайн: сайт. **–** URL: www.convertworld.com.
6. Elibrary.ru. Научная электронная библиотека: официальный сайт. – URL: www.elibrary.ru.
7. Глобус –Телеком: официальный сайт. **–** URL: http:/www.globus-telecom.com. Морион. Российский разработчик и производитель оборудования связи. **–** URL: http://www.morion.ru/.
8. НАТЕКС: официальный сайт. **–** URL: http://www.nateks.ru/.
9. ISKRATEL: официальный сайт. **–** URL: http://www.iskratel.com/.
10. Промсвязь: официальный сайт **–** URL: http://www.ps-ufa.ru/.
11. 3M. Наука, воплощенная в жизнь. **–** URL: http://3m.com/; https://www.3mrussia.ru/.
12. ОАО «Ферроприбор». **–**URL: http://www.rusgates.ru/index/php
13. Connect! Мир связи: сетевой журнал. **–** URL: http://www.connect.ru/.
14. RusCable.Ru. Энергетика. Электротехника. Связь: отраслевое электронное СМИ. **–** URL: http://www.ruscable.ru/. – Текст: электронный.
15. ГП Телеком: официальный сайт **–** URL: http://www.gptelecom.ru/.
16. Компоненты и технологии: сетевой журнал. **–** URL: http://www.kit-e.ru/.
17. Открытые системы. **–** URL: http://www.osp.ru/.
18. Сети и системы связи: архив журнала. – URL: http://www.ccc.ru/.
19. Современные телекоммуникации России: отраслевой информационно-аналитический онлайн-журнал. – URL: http://www.telecomru.ru/.
20. Электросвязь: сайт журнала. – URL: <http://www.elsv.ru/>.
21. Энциклопедия инструментов: иллюстрированный справочник по инструментам и приборам. – URL: <http://www.tools.ru/tools.htm>.
22. Зингеренко, Ю.А. Оптические цифровые телекоммуникационные системы и сети синхронной цифровой иерархии: учебное пособие/Ю.А.Зингеренко. - СПб.: НИУ ИТМО, 2013. **–** URL: http://window.edu.ru/resource/440/80440.
23. Иванов, В.И. Волоконно-оптические системы передачи: /ВИ.Иванов; Поволжский гос. университет телекоммуникаций и информатики. - Самара: ПГУТИ, 2011. **–** URL: https://vk.cc/8xhCn0.
24. Марусина, М.Я. Метрологическое обеспечение средств измерений: учебное пособие М.Я.Марусина, В.Л.Ткалич, Р.Я.Лабковская. – СПб: Университет ИТМО, 2019. https://books.ifmo.ru/file/pdf/2422.pdf
25. Трошин, А.В. Цифровые системы передачи: учебное пособие/А.В.Трошин; Поволжский гос. ун-т телекоммуникаций и информатики. – Текст: электронный. - Самара: ГОУВПО ПГУТИ, 2013. **–** URL: https://vk.cc/8xhH2k.

**Приложения**

**Приложение А**

**Форма титульного листа отчета по практике**

Федеральное государственное образовательное бюджетное учреждение высшего образования

**Финансовый университет при Правительстве Российской Федерации**

**(Липецкий филиал)**

Кафедра информационных систем и программирования

**ОТЧЕТ**

производственной практики (по профилю специальности)

на материалах \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

наименование профильной организации

Студента \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ФИО студента

Группа \_\_\_\_\_\_\_\_\_\_\_

Специальность: 10.02.04. Обеспечение информационной безопасности телекоммуникационных систем

Руководитель практики

от Липецкого филиала \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_

ФИО подпись

Руководитель практики

от профильной организации \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_

ФИО подпись

Оценка \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

М.П.

Липецк – 20\_\_\_ г.

**Приложение Б**

**Форма дневника прохождения практики**

Федеральное государственное образовательное бюджетное учреждение высшего образования

**Финансовый университет при Правительстве Российской Федерации**

**(Липецкий филиал)**

Кафедра информационных систем и программирования

**ДНЕВНИК**

производственной практики (по профилю специальности) студента

Студента \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ФИО студента

Курс \_\_\_\_\_\_\_\_\_\_

Группа \_\_\_\_\_\_\_\_\_\_\_

Место проведения практики: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Специальность: 10.02.04. Обеспечение информационной безопасности телекоммуникационных систем

Руководитель практики

от Липецкого филиала \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_

ФИО подпись

Руководитель практики

от профильной организации \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_

ФИО подпись

Начало практики

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_\_ года

Окончание практики

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_\_ года

Липецк – 20\_\_\_ г.

Таблица 1 - График проведения практики

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№** | **Содержание мероприятий и их вид** | **Кол-во часов** | **Дата** | **ФИО, должность консультанта, лектора** | **Подпись руководителя практики от предприятия** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| … |  |  |  |  |  |
| n |  |  |  |  |  |

Примечание:

* график проведения практики согласовывается с руководителем практики от предприятия и от филиала.
* отчет оформляется в процессе прохождения практики;
* к отчету о прохождении практики прикладывается заверенный печатью отзыв руководителя практики от предприятия, характеризующий студента и результаты, полученные им в ходе прохождения практики;
* сдача зачета по практике – по окончанию срока прохождения практики;
* подписи руководителя со стороны предприятия на титульном листе отчета и в дневнике должны быть также заверены печатью организации.