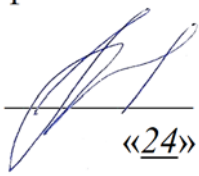
Федеральное государственное образовательное бюджетное
учреждение высшего образования
«Финансовый университет при Правительстве Российской Федерации»
(Финансовый университет)
Липецкий филиал Финуниверситета

УТВЕРЖДАЮ
Заместитель директора
по учебно-методической работе
Липецкого филиала Финуниверситета



О.Н. Левчегов
«*24*» *апреля* 20*24* г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

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 23.04.2024 г. №10

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 профессиональным модулям: ПМ.01. Эксплуатация информационно-телекоммуникационных систем и сетей, ПМ.02. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты, ПМ.03. Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты, ПМ.04. Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих.

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;

– программ профессиональных модулей ПМ.01. Эксплуатация информационно-телекоммуникационных систем и сетей, ПМ.02. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты, ПМ.03. Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты, ПМ.04. Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих.

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

Иметь практический опыт	О1 – монтажа, настройки, проверки функционирования и конфигурирования оборудования информационно-телекоммуникационных систем и сетей (ИТКС); О2 – текущего контроля функционирования оборудования ИТКС; О3 – проведения технического обслуживания, диагностики технического состояния, поиска неисправностей и ремонта оборудования ИТКС; 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. О10 – выявление технических каналов утечки информации; О11 – использование основных методов и средств инженерно-технической защиты информации; О12 – диагностики, устранения отказов и восстановления работоспособности инженерно- технических средств обеспечения информационной безопасности; О13 – участие в мониторинге эффективности инженерно-технических средств обеспечения информационной безопасности; О14 – решение частных технических задач, возникающих при аттестации объектов, помещений, технических средств.

	О15 – выполнения технологического процесса сборки, монтажа и демонтажа узлов, блоков, приборов и устройств радиоэлектронной аппаратуры в соответствии с технической документацией;
Уметь	У1 – осуществлять техническую эксплуатацию линейных сооружений связи; У2 – производить монтаж кабельных линий и оконечных кабельных устройств; У3 – настраивать, эксплуатировать и обслуживать оборудование ИТКС; У4 – осуществлять подключение, настройку мобильных устройств и распределенных сервисов ИТКС; У5 – производить испытания, проверку и приемку оборудования телекоммуникационных систем; У6 – проводить работы по техническому обслуживанию, диагностики технического состояния и ремонту оборудования ИТКС; У7 – измерять основные качественные показатели и характеристики при выполнении профилактических и ремонтных работ приемо-передающих устройств (ППУ); У8 – читать принципиальные схемы блоков ППУ; У9 – выполнять расчеты, связанные с определением значений параметров режима и элементов ППУ; У10 – контролировать работу и осуществлять техническую эксплуатацию ППУ; У11 – настраивать, эксплуатировать и обслуживать локальные вычислительные сети; У12 – сопрягать между собой различные телекоммуникационные устройства; У13 – производить настройку программного обеспечения коммутационного оборудования телекоммуникационных систем; У14 – осуществлять настройку модемов, используемых в защищенных телекоммуникационных системах; У15 – проверять функционирование, производить регулировку и контроль основных параметров источников питания радиоаппаратуры; У16 – проводить типовые измерения; У17 – пользоваться стандартными средствами электрорадиоизмерений; У18 – оценивать точность проводимых измерений; У19 – оформлять эксплуатационную и ремонтную документацию. 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. У27 – применять технические средства защиты информации; У28 – использовать средства охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения; У29 – использовать средства защиты информации от несанкционированного съема и утечки по техническим каналам;

	У30 – применят нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности техническими средствами. У31 – читать маркировку электрорадиоэлементов. читать электрические принципиальные схемы. У32 – пользоваться технологической документацией при изготовлении радиоэлектронной аппаратуры; У33 – формировать, устанавливать и крепить электронные элементы на печатные платы; У34 – проводить монтаж электронных элементов на печатных платах; У35 – контролировать качество пайки; производить сборку лицевых панелей приборов; У36 – крепить жгуты, кабели и провода к платам и шасси приборов; У37 – пользоваться инструментом и приспособлениями для сборки аппаратуры; У38 – осуществлять визуальный, электрический и механический контроль монтажа.
Знать	З1 – принципы построения информационно-телекоммуникационных систем и сетей; З2 – базовые технологии построения и состав оборудования мультисервисных сетей связи; З3 – состав и основные характеристики типового оборудования ИТКС; З4 – принципы передачи информации в ИТКС; З5 – принцип модуляции сигналов ИТКС; З6 – принципы помехоустойчивого кодирования сигналов ИТКС; З7 – виды и характеристики сигналов в ИТКС; З8 – принципы аналого-цифрового преобразования, работы компандера, кодера и декодера; З9 – особенности распространения электромагнитных волн различных диапазонов частот; З10 – виды помех в каналах связи, методы защиты от них; З11 – разновидности проводных линий передачи; З12 – конструкцию и характеристики электрических и оптических кабелей связи; З13 – способы коммутации в сетях связи; З14 – принципы построения многоканальных систем передачи; З15 – принципы построения радиолиний и систем радиосвязи; З16 – основы маршрутизации в информационно-телекоммуникационных сетях; З17 – принципы построения, основные характеристики и оборудование систем подвижной радиосвязи; З18 – технологии и оборудование удаленного доступа в информационно - телекоммуникационных сетях; З19 – типовые услуги, предоставляемые с использованием информационно-телекоммуникационных сетей, виды информационного обслуживания, предоставляемые пользователям; З20 – принципы построения и технические средства локальных сетей; З21 – принципы функционирования маршрутизаторов; З22 – модемы, использующиеся в ИТКС, принципы подключения и функционирования; З23 – спецификацию изделий, комплектующих, запасного имущества и ремонтных материалов, порядок их учета и хранения; З24 – принципы организации эксплуатации ИТКС; З25 – содержание технического обслуживания и восстановления работоспособности оборудования ИТКС;

	З26 – принципы организации и технологию ремонта оборудования ИТКС; З27 – периодичность поверок контрольно-измерительной аппаратуры; З28 – принцип действия выпрямителей переменного тока; З29 – принципы работы стабилизаторов напряжения и тока, импульсных источников питания. З30 – принципы защиты электронных устройств от недопустимых режимов работы; З31 – принципы построения, основные характеристики типовых измерительных приборов и правила работы с ними; З32 – основные понятия и определения метрологии, стандартизации и сертификации. 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. З40 – физику возникновения технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; З41 – номенклатуру и характеристики аппаратуры, используемой для съема, перехвата и анализа сигналов в технических каналах утечки информации; З42 – основные методы и средства технической защиты информации, номенклатуру применяемых средств защиты информации от несанкционированного съема и утечки по техническим каналам; З43 – номенклатуру применяемых средств охраны объектов, систем видеонаблюдения. З44 – основные сведения о профессии монтажника радиоэлектронной аппаратуры и приборов; З45 – принципы организации рабочего места; З46 – основные виды электрорадиоэлементов и конструктивных деталей, марки проводов и кабелей, применяемых при монтаже радиоаппаратуры; З47 – основные требования, предъявляемые к электрическому монтажу, установке и креплению навесных электрорадиоэлементов и конструктивных деталей при объемном и печатном монтаже; З48 – назначение и применение изоляционных материалов, основных видов припоев и флюсов. З49 – способы пайки и предъявляемые к ней требования, особенности пайки полупроводниковых приборов и микросхем; З50 – назначение приспособлений, контрольно-измерительных инструментов и приборов, правила пользования ими; З51 – строго выполнять мероприятия по охране труда и противопожарной защите при выполнении сборочных и электромонтажных работ.

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)

7. Перечень типовых контрольных вопросов, задаваемых при защите отчета о прохождении производственной практики (по профилю специальности)

– Структура подразделений, основ документооборота и организации передачи информации у оператора связи;
– Методы передачи информации, используемые оператором связи, характер и интенсивность информационных процессов;
– Угрозы информационной безопасности и методами решения задач по защите информации у оператора связи;
– Технологии защиты информации, внедрённые на предприятии оператора связи;

- Системы управления процессами передачи информации и защиты информации у оператора связи;
- Какие используются на предприятии оператора связи методы и средства управления процессами передачи информации;
- Понятие и сфера действия конфиденциального делопроизводства.
- Основные задачи организации конфиденциального делопроизводства.
- Цели защиты конфиденциальной информации.
- Основные понятия, виды и источники информации, подлежащей защите
- Виды конфиденциальных документов
- Причины, классификация и характеристики каналов утечки конфиденциальной информации

Список использованной литературы

1. Федеральный закон «О техническом регулировании». **й.** – 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.

1. ГОСТ Р 8.563-2009 Государственная система обеспечения единства измерений (ГСИ). Методики (методы) измерений. –URL: http://docs.cntd.ru/document/1200077909.
7. ГОСТ Р 8.000-2015 Государственная система обеспечения единства измерений (ГСИ). Основные положения. –URL: http://docs.cntd.ru/document/1200124116.
8. ОСТ 45.150-99 Отраслевая система обеспечения единства измерений. Методики выполнения измерений. Порядок разработки и аттестации. – URL: http://docs.cntd.ru/document/1200036493.
9. ГОСТ Р 40.002-2000 Система сертификации ГОСТ Р. Регистр систем качества. Основные положения. –URL: http://docs.cntd.ru/document/1200006218.
10. ГОСТ Р 1.0-92 Государственная система стандартизации РФ. Основные положения. – URL: http://docs.cntd.ru/document/5200306.

Электронные издания:

11. Нефедов, В.И. Теория электросвязи: учебник для студ. учрежд. СПО /В.И.Нефедов, А.С.Сигов. - Москва: Юрайт, 2020.
12. Ситников, А. В. Электротехнические основы источников питания: учебник для студ. учрежд. СПО/ А.В. Ситников, И.А. Ситников. - Москва: КУРС: ИНФРА-М, 2020.
13. Хрусталева, З.А. Метрология, стандартизация и сертификация. Практикум: учебное пособие для студ. учрежд. СПО/ З.А.Хрусталева. - Москва: КноРус, 2020.
14. Шишмарёв, В.Ю. Метрология, стандартизация, сертификация, техническое регулирование и документоведение: учебник для студ. учрежд. СПО/В.Ю.Шишмарев. – Москва: КУРС: ИНФРА-М, 2020.
15. 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:

16. 1. Федеральное агентство связи (Россвязь): официальный сайт. Документы. – URL: https://rossvyaz.gov.ru/dokumenty.
17. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации: официальный сайт. – URL: http://www.minsvyaz.ru/.
18. Федеральная служба по техническому и экспортному контролю (ФСТЭК России): официальный сайт. – URL: www.fstec.ru.
19. Информационно- коммуникационные технологии в образовании: федеральный портал. – URL: htpp\\:www.ict.edu.ru.
20. Convertworld.com. Перевод единиц измерения онлайн: сайт. – URL: www.convertworld.com.
21. Elibrary.ru. Научная электронная библиотека: официальный сайт. – URL: www.elibrary.ru.
22. Глобус –Телеком: официальный сайт. – URL: http:/www.globus-telecom.com. Морион. Российский разработчик и производитель оборудования связи. – URL: http://www.morion.ru/.

23. НАТЕКС: официальный сайт. – URL: http://www.nateks.ru/.
24. ISKRATEL: официальный сайт. – URL: http://www.iskratel.com/.
25. Промсвязь: официальный сайт – URL: http://www.ps-ufa.ru/.
26. 3М. Наука, воплощенная в жизнь. – URL: http://3m.com/; https://www.3mrussia.ru/.
27. ОАО «Ферроприбор». –URL: http://www.rusgates.ru/index/php
28. Connect! Мир связи: сетевой журнал. – URL: http://www.connect.ru/.
29. RusCable.Ru. Энергетика. Электротехника. Связь: отраслевое электронное СМИ. – URL: http://www.ruscable.ru/. – Текст: электронный.
30. ГП Телеком: официальный сайт – URL: http://www.gptelecom.ru/.
31. Компоненты и технологии: сетевой журнал. – URL: http://www.kit-e.ru/.
32. Открытые системы. – URL: http://www.osp.ru/.
33. Сети и системы связи: архив журнала. – URL: http://www.ccc.ru/.
34. Современные телекоммуникации России: отраслевой информационно-аналитический онлайн-журнал. – URL: http://www.telecomru.ru/.
35. Электросвязь: сайт журнала. – URL: http://www.elsv.ru/.
36. Энциклопедия инструментов: иллюстрированный справочник по инструментам и приборам. – URL: http://www.tools.ru/tools.htm.
37. 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.
38. Иванов, В.И. Волоконно-оптические системы передачи: /ВИ.Иванов; Поволжский гос. университет телекоммуникаций и информатики. - Самара: ПГУТИ, 2011. – URL: https://vk.cc/8xhCn0.
39. 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
40. 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
1.					
2.					
3.					
…					
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.