Министерство науки и высшего образования Российской Федерации
федеральное государственное бюджетное образовательное учреждение высшего образования
«Российский экономический университет им. Г.В. Плеханова»
Московский приборостроительный техникум

РАБОЧАЯ ПРОГРАММА

Производственная практика (преддипломная)

специальность:
10.02.05 Обеспечение информационной безопасности автоматизированных систем

квалификация:
техник по защите информации

очная форма обучения

2022

СОГЛАСОВАНА:
Цикловой методической комиссией
«10.02.05 Профессиональных модулей»

Протокол № 6-21/22 ЗК
от «15» января 2022 года

Разработана на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования
специальность: 10.02.05 Обеспечение информационной безопасности автоматизированных систем
квалификация: техник по защите информации

Председатель цикловой методической комиссии

Подпись **М.А. Молотков**
Инициалы Фамилия

Заместитель директора по учебной работе

Подпись **Д.А. Клопов**
Инициалы Фамилия

УТВЕРЖДЕНА:
Директор техникума

Подпись **А.В. Чурилов**
Инициалы Фамилия

Составители (авторы):
Прищеп Михаил Сергеевич, преподаватель ФГБОУ ВО РЭУ им. Г.В. Плеханова
Молотков Максим Алексеевич, преподаватель ФГБОУ ВО РЭУ им. Г.В. Плеханова

Кузнецов Павел Олегович, преподаватель ФГБОУ ВО РЭУ им. Г.В. Плеханова

СОГЛАСОВАНО: Ахмадиев С.Г.
представитель работодателя

Рецензент: _____
Ф.И.О., ученая степень, звание, должность, наименование

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)

1.1. Область применения программы практики

Производственная практика (преддипломная) проводится в соответствии с федеральным государственным образовательным стандартом среднего профессионального образования программы подготовки специалистов среднего звена специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем и является частью образовательного процесса.

Преддипломная практика является завершающим этапом обучения и проводится после прохождения общего гуманитарного и социально-экономического, математического и общего естественнонаучного, профессионального, и разделов: учебная практика; производственная практика (по профилю специальности) и промежуточных аттестаций.

Преддипломная практика направлена на углубление студентом первоначального профессионального опыта, развитие общих и профессиональных компетенций, проверку его готовности к самостоятельной трудовой деятельности, а также на подготовку к выполнению выпускной квалификационной работы (дипломного проекта или дипломной работы) в организациях различных организационно-правовых форм (далее - организация). Преддипломная практика проводится непрерывно после освоения учебной практики и практики по профилю специальности.

Преддипломная практика способствует дальнейшему развитию практических навыков по следующим видам деятельности: обработка информации, разработка, внедрение, адаптация, сопровождение программного обеспечения и информационных ресурсов, наладка и обслуживание оборудования отраслевой направленности в производственных, обслуживающих, торговых организациях, административно-управленческих структур (по отраслям).

Объектами профессиональной деятельности выпускников являются:

- информация;
- информационные процессы и информационные ресурсы;
- языки и системы программирования контента, системы управления контентом;
- средства создания и эксплуатации информационных ресурсов;
- программное обеспечение;
- оборудование: компьютеры и периферийные устройства, сети, их комплексы и системы отраслевой направленности;
- техническая документация;
- первичные трудовые коллективы.

Техник по защите информации готовится к следующим видам деятельности:

- Эксплуатация автоматизированных (информационных) систем в защищённом исполнении;
- Защита информации в автоматизированных системах программными и программно-аппаратными средствами;
- Защита информации техническими средствами;
- Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих.

а также для подготовки студентов к осознанному выполнению выпускной квалификационной работы.

Началу практики должен предшествовать выбор темы дипломного проекта (работы). По завершении практики тема дипломного проекта (работы) может уточняться.

Темы дипломных проектов (работ) рассматриваются и принимаются на заседании цикловой методической комиссии и утверждаются зам. директора по учебной работе.

Закрепление темы и назначение руководителя дипломного проекта утверждаются приказом, согласованным с заместителем по учебной работе. Корректировка темы и/или

руководителя дипломного проекта допускается в исключительных случаях на основе письменного заявления студента, служебной записки руководителя дипломного проекта или результатов предзащиты. Изменения утверждаются приказом.

Практикант совместно с руководителем оформляет задание на ВКР, утверждаемое председателем ЦМК Профессиональных модулей. В задании определяется график выполнения работ (Приложение №1).

До практики проводится собрание, на котором доводятся цели, содержание, объем работ, правила прохождения практики. Срок проведения практики устанавливается в соответствии с учебным планом.

Руководителями практики назначаются, как правило, руководители дипломной работы, утвержденные на заседании ЦМК. Руководитель оказывает студенту консультационную и методическую помощь в организации работы, изучении предметной области, специальной литературы, по поставленной проблеме, сбору материалов к дипломной работе.

Часть преддипломной практики отводится на самостоятельную работу студента. К самостоятельной работе можно отнести:

1) Оформление отчетной документации;
2) Документирование процессов на производстве;
3) Анализ деятельности предприятия;
4) Ознакомление с производственными процессами;
5) Изучение направления работы организации.

Продолжительность преддипломной практики — 4 недели. Практику проходят студенты очной формы обучения. В последний день производственной практики (преддипломной) студент обязан предоставить:

1) отзыв руководителя преддипломной практики;
2) дневник прохождения практики установленного образца;
3) письменный отчет студента о прохождении практики;
4) черновые материалы результата проектирования;
5) результаты экспериментальных работ.

1.2. Цели и задачи практики – требования к результатам освоения практики, формы отчетности

Производственная практика (преддипломная) студентов является заключительной частью образовательного процесса и направлена на закрепление и углубление компетенций, полученных студентами в процессе всего предыдущего обучения, а также на углубление студентом первоначального профессионального опыта, развитие общих и профессиональных компетенций и опытом профессиональной деятельности по получаемой специальности.

Задачами преддипломной практики являются:

1) обобщение и совершенствование знаний и практических навыков, полученных студентами в процессе обучения по специальности;
2) проверка возможностей самостоятельной работы будущего специалиста в условиях конкретного производства;
3) сбор материала для выполнения дипломного проекта.

Реализация цели и задач практики должна осуществляться с учетом сферы деятельности организации или предприятия.

По окончании практики студент сдаёт отчет в соответствии с содержанием тематического плана практики и по форме, установленной в МПТ ФГБОУ ВО «РЭУ им. Г.В. Плеханова».

Итоговая аттестация проводится в форме - **дифференцированного зачёта.**

1.3. Количество часов на освоение программы практики

Рабочая программа практики рассчитана на прохождение студентами практики в объеме **144** часов.

Базами практики являются организации различных организационно-правовых форм и форм собственности, оснащённые современным оборудованием, обеспеченные квалифицированным персоналом. Практика проводится в организациях на основе прямых договоров, заключаемых между техникумом и организациями.

2. РЕЗУЛЬТАТЫ ПРАКТИКИ

Преддипломная практика направлена на углубление студентом первоначального профессионального опыта, развитие общих и профессиональных компетенций, соответствующим видам деятельности:

Вид деятельности	Код	Наименование профессиональных компетенций
Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	ПК 1.1.	Производить установку и настройку компонентов автоматизированных (информационных систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
	ПК 1.2.	Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.
	ПК 1.3.	Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
	ПК 1.4.	Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.
Защита информации в автоматизированных системах программными и программно-аппаратными средствами;	ПК 2.1	Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.
	ПК 2.2	Обеспечивать защиту информации в автоматизированных системах отдельными программами, программно-аппаратными средствами.
	ПК 2.3.	Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.
	ПК 2.4.	Осуществлять обработку, хранение и передачу информации ограниченного доступа.
	ПК 2.5.	Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.
	ПК 2.6	Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных программно-аппаратных средств обнаружения, предупреждения и ликвидации последствии компьютерных атак.
Защита информации техническими средствами;	ПК 3.1.	Осуществлять установку, монтаж, настройку т техническое обслуживание технических средств информации в соответствии с требованиями эксплуатационной документации.

	ПК 3.2.	Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации
	ПК 3.3.	Осуществлять изменение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа.
	ПК 3.4.	Осуществлять изменение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.
	ПК 3.5.	Организовывать отдельные работы по физической защите объектов информации.
Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих.	ПК 4.1.	Производить инсталляцию, настройку и обслуживание программного обеспечения компьютерных систем.
	ПК 4.2.	Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах.
	ПК 4.3.	Выполнять работы по модификации отдельных компонент программного обеспечения.
	ПК 4.4.	Обеспечивать защиту программного обеспечения компьютерных систем.
	ПК 4.5.	Проводить аудит систем безопасности баз данных и серверов, с использованием регламентов по защите информации.

Общие компетенции:

Код	Наименование общих компетенций
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности
ОК 09	Использовать информационные технологии в профессиональной деятельности
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языках

Аттестация по итогам практики проводится в форме дифференцированного зачета, на основании оформленного в соответствии с установленными требованиями отчета, отзыва руководителя практики, представленных материалов, а также устного доклада. Принимает зачет руководитель дипломного проекта. По итогам аттестации выставляется оценка (отлично, хорошо, удовлетворительно, неудовлетворительно).

К студенту, не выполнившему программу практики и задание в установленный срок, получившему отрицательный отзыв руководителя или неудовлетворительную оценку при защите, применяются санкции как к неуспевающему студенту, вплоть до отчисления из техникума.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИКИ

3.1. Тематический план практики

Наименование профессионального модуля	Коды формируемых компетенций	Объем времени, отводимый на практику	Сроки проведения практики
Производственная практика (преддипломная)	ПК 1.1 – ПК 1.4	4 недели – 144 часа	В соответствии с графиком учебного процесса, с 20 апреля по 17 мая.
	ПК 2.1 – ПК 2.6		
	ПК 3.1 – ПК 3.5		
	ПК 4.1 – ПК 4.5		

3.2. Содержание производственной практики (преддипломной)

- консультации со специалистами-практиками по теме дипломного проекта;
- изучение исходной информации по теме дипломного проекта:

1. исследование предметной области дипломного проекта;
2. проведение моделирования объектов предметной области и их взаимосвязи;
3. выбор методов и средств решения задачи моделирования;
4. изучение существующих информационных технологий и систем информационного обеспечения для решения реальных задач организационной, управленческой или научной деятельности в условиях конкретных производств, организаций или фирм;
5. выполнение работ в качестве исполнителя или стажера на автоматизированном рабочем месте;
6. формулировка требований по предмету дипломного проекта;

- выполнение предварительного проектирования, на предмет выбора лучшей структуры программы и данных;
- выполнение экспериментальных работ по программированию в части поиска лучшего решения: структуры ядра и основных блоков программы.
-

Наименование разделов и тем	Содержание освоенной учебной информации, виды работ, выносимые на практику в соответствии с рабочими программам профессиональных модулей	Объем часов	ПК
Вводное занятие	**Содержание выполняемых работ**	**4**	
	1. Ознакомление с содержанием, видами и порядком выполняемых работ 2. Инструктаж по прохождению практики и правилам безопасности работы на предприятии		ПК 1.1 – ПК 1.4 ПК 2.1 – ПК 2.6 ПК 3.1 – ПК 3.5 ПК 4.1 – ПК 4.5
Тема 1. Формирование требований	**Содержание выполняемых работ**	**22**	
	1. Обследование объекта и подготовительная работа с экспертами 2. Обоснование необходимости создания или модификации ИС в защищенном исполнении 3. Формирование требований к пользователям ИС 4. Оформление документации о выполнении работ и заявки на разработку ИС		ПК 1.1 – ПК 1.4 ПК 2.1 – ПК 2.6 ПК 3.1 – ПК 3.5 ПК 4.1 – ПК 4.5
	Содержание выполняемых работ	**36**	

Тема 2. Разработка концепции ИС	1. Изучение объекта с точки зрения функциональной и организационной структуры 2. Изучение объекта с точки зрения организации и содержания документооборота 3. Проведение необходимых научно-исследовательских работ 4. Разработка вариантов концепции ИС 5. Выбор варианта концепции ИС, удовлетворяющего требованиям пользователей 6. Оформление документации о проделанной работе		ПК 1.1 – ПК 1.4 ПК 2.1 – ПК 2.6 ПК 3.1 – ПК 3.5 ПК 4.1 – ПК 4.5
Тема 3. Техническое задание	**Содержание выполняемых работ**	**16**	
	1. Разработка и утверждение плана технического задания на создание или модификацию ИС в защищенном исполнении 2. Детализация разделов плана технического задания на создание или модификацию ИС в защищенном исполнении 3. Утверждение технического задания на создание ИС в защищенном исполнении		ПК 1.1 – ПК 1.4 ПК 2.1 – ПК 2.6 ПК 3.1 – ПК 3.5 ПК 4.1 – ПК 4.5
Тема 4. Эскизный проект	**Содержание выполняемых работ**	**18**	
	1. Обоснование предварительных проектных решений по отдельным частям ИС 2. Обоснование предварительных проектных решений по ИС в целом 3. Разработка предварительных проектных решений по отдельным частям ИС в защищенном исполнении 4. Разработка предварительных проектных решений по ИС в целом 5. Разработка документации на ИС в целом и на ее отдельные части		ПК 1.1 – ПК 1.4 ПК 2.1 – ПК 2.6 ПК 3.1 – ПК 3.5 ПК 4.1 – ПК 4.5
Тема 5 Технический проект	**Содержание выполняемых работ**	**26**	
	1. Разработка проектных решений по отдельным частям ИС в защищенном исполнении 2. Разработка проектных решений по ИС в целом 3. Разработка и оформление документации		ПК 1.1 – ПК 1.4 ПК 2.1 – ПК 2.6 ПК 3.1 – ПК 3.5 ПК 4.1 – ПК 4.5
Тема 6 Рабочая документация	**Содержание выполняемых работ**	**16**	
	1. Разработка рабочей документации на внедрение ИС 2. Разработка документации по техническому сопровождению ИС в период эксплуатации 3. Разработка документации по обучению пользователей работе с ИС 4. Формирование справочной интерактивной поддержки ИС 5. Создание или адаптация Интернет-ресурса поддержки ИС 6. Разработка и оформление документации		ПК 1.1 – ПК 1.4 ПК 2.1 – ПК 2.6 ПК 3.1 – ПК 3.5 ПК 4.1 – ПК 4.5

Итоговая аттестация	1. Оформление отчетной документации по преддипломной практике 2. Представление отчета в соответствии с содержанием тематического плана практики и по установленной форме 3. Разработка и оформление документации	6	
Всего		144	

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРАКТИКИ

4.1. Требования к документации, необходимой для проведения практики

Для проведения практики в техникуме разработана следующая документация:

– положение об учебной и производственной практике студентов;
– рабочая программа практики;
– календарно-тематический план;
– приказ о назначении руководителя практики от образовательного учреждения
– приказ о закреплении темы выпускной квалификационной работы в форме дипломного проекта (работы)
– договоры с предприятиями по проведению практики;
– приказ о распределении студентов по базам практики;
– план-график консультаций и контроля за выполнением студентами программы практики (при проведении практики на предприятии);
– график защиты отчетов по практике.

4.2. Требования к учебно-методическому обеспечению практики

В целях реализации требований к учебно-методическому обеспечению практики разработаны и утверждены:

– Задания на практику;
– Методические рекомендации для студентов по выполнению видов работ на практике;
– Методические рекомендации по формированию отчетов по практике;
– Методические рекомендации по оформлению дневника по практике;
– Критерии оценки прохождения практики и защиты отчетов.

4.3. Требования к студенту-практиканту:

При прохождении практики студент обязан:

- руководствоваться программой практики;
- в полном объеме выполнять задания и рекомендации руководителя практики;
- строго соблюдать действующие на предприятии (в организации) правила внутреннего распорядка;
- строго соблюдать правила охраны труда, техники безопасности и производственной санитарии;
- поддерживать имидж предприятия;
- сохранять коммерческую тайну предприятия;
- ответственно относиться к выполнению производственных обязанностей и заданий;
- быть достойным представителем ФГБОУ ВО «РЭУ им. Г.В. Плеханова» на предприятиях различной форм собственности.

4.4. Требования к отчетным документам

1. Дневник ведётся ежедневно и заполняется кратким описанием работы. Из содержания дневника должны быть видны: проделанная студентом работа, техническая характеристика объекта работы. По данным дневника одновременно ведётся составление отчёта о практике в соответствии с планом и программой практики.

2. Отчёт должен оформляться в последние дни пребывания студента-практиканта на месте практики. Рекомендуемый объект отчёта – от 7 до 10 стандартных страниц текста (с использованием рисунков, фотографий, схем). Основу содержания отчёта должны составлять: самостоятельные личные наблюдения, критический анализ, составление и оценка действующих технических средств, процессов и организации работ, а также личные рационализаторские предложения, выводы и заключения.

3. Дневник и отчёт должны быть полностью закончены на месте практики и представлены для заключения и составления отзыва о прохождении практики студентом руководителю производственной практики от организации.

4. Отзыв о работе студента-практиканта составляется руководителем практики от организации на фирменном бланке с указанием оценки (по пятибалльной системе), за подписью руководителя организации или руководителя практики, заверенной оттиском печати.

5. Студент-практикант представляет подписанные документы (отчёт, отзыв и дневник по практике) руководителю практики от техникума на следующий день после завершения практики.

4.5. Требования к материально-техническому обеспечению практики

Преддипломная практика студентов должна проходить в одном из подразделений предприятия (организации, учреждения), выполняющего экономические, плановые, организационные или управленческие функции, или их комплекс с применением информационных технологий. Имея рабочее место в одном из таких подразделений, студенты знакомятся с деятельностью других подразделений по мере выполнения программы практики.

Во время прохождения практики студенты соблюдают и выполняют все требования, действующие на предприятии, правила внутреннего трудового распорядка. На время практики студент может быть принят на вакантную штатную должность с выполнением конкретного производственного задания и оплатой труда. В этом случае на него распространяются все положения трудового законодательства и положения соответствующей должностной инструкции.

Организация и учебно-методическое руководство преддипломной практикой студентов осуществляется выпускающей цикловой методической комиссией. Ответственность за организацию практики на предприятии возлагается на специалистов в области управления производством, назначенных руководством предприятия.

Студенты направляются на места практики в соответствии с договорами, заключенными с базовыми предприятиями и организациями, или по запросу предприятий.

За студентами, зачисленными на период практики на штатную оплачиваемую должность, сохраняется стипендия. При нарушении студентом трудовой дисциплины и правил внутреннего распорядка предприятия по представлению руководителя подразделения и руководителя практики от предприятия он может быть отстранен от прохождения практики, о чем сообщается заведующему отделением и председателю выпускающей цикловой методической комиссии. По их предложению директор может рассматривать вопрос об отчислении студента из техникума.

Оборудование рабочих мест

- нормативно-правовая документация
  - комплект бланков проектной документации;
  - комплект учебно-методической документации;
  - наглядные пособия.
- методическое обеспечение лабораторных и практических работ, тесты;
- лицензионное программное обеспечение;

Оборудование

- компьютер,
- принтер,
- сканер,
- модем (спутниковая система),
- программное обеспечение общего и профессионального назначения,

базовые:

- операционные системы (две основные линии развития ОС (открытые и закрытые);
- инструментальная среда для разработки проекта;
- программные среды (текстовые процессоры, электронные таблицы, персональные информационные системы, программы презентационной графики, браузеры, редакторы

WEB-страниц, почтовые клиенты, редакторы растровой графики, редакторы векторной графики, настольные издательские системы, средства разработки);

прикладные:

- информационные системы по отраслям применения (корпоративные, экономические, медицинские и др.);
- автоматизированного проектирования (CASE-технологии, CAD, CAM, CAE, MPM, BOM, CRM-системы).

4.6. Информационное обеспечение обучения.

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

ПМ.01:

4.6.1 Печатные издания
ОСНОВНЫЕ ***не используются***
ДОПОЛНИТЕЛЬНЫЕ ***не используются***

4.6.2 Электронные издания
ОСНОВНЫЕ

1. Костров Б.В. Сети и системы передачи информации (2-е изд.), М. Академия, 2019 https://academia-library.ru/catalogue/4831/408564/
2. Мельников Д. Информационная безопасность открытых систем. - М.: Форум, 2019. https://znanium.com/bookread2.php?book=1042499
3. Синицын С.В., Батаев А.В., Налютин Н.Ю. Операционные системы – М.: Издательский центр «Академия», 2016. https://www.book.ru/view4/917804/1
4. Скрипник Д. А. Общие вопросы технической защиты информации: учебное пособие / Скрипник Д. А. –М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. http://biblioclub.ru/index.php?page=book&id=429070

ДОПОЛНИТЕЛЬНЫЕ

1. Партыка Т. Л., Попов И. И. Операционные системы, среды и оболочки: учеб. пос. для студентов СПО – М.: Форум, 2017. – 544 с

   https://znanium.com/bookread2.php?book=552493

4.6.3. Периодические издания:

1. Журналы Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей;
2. Журналы Защита информации. Инсайд: Информационно-методический журнал
3. Информационная безопасность регионов: Научно-практический журнал
4. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности. URL: http://cyberrus.com/
5. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: http://bit.mephi.ru/

4.6.4. Электронные ресурсы:

1. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
2. Информационный портал по безопасности www.SecurityLab.ru.
3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
4. Российский биометрический портал www.biometrics.ru
5. Сайт журнала Информационная безопасность http://www.itsec.ru –
6. Сайт Научной электронной библиотеки www.elibrary.ru
7. Справочно-правовая система «Гарант» » www.garant.ru
8. Справочно-правовая система «Консультант Плюс» www.consultant.ru
9. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
10. Федеральный портал «Информационно-коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru
11. Федеральный портал «Российское образование www.edu.ru

4.6.5 Профессиональные базы данных и справочные системы

- Федеральная служба государственной статистики - https://rosstat.gov.ru/
- Наукометрическая и реферативная база данных SCOPUS - https://www.scopus.com
- Информационно-справочная система "КонсультантПлюс"

ПМ.02:

4.6.1 Печатные издания

ОСНОВНЫЕ ***не используются***

ДОПОЛНИТЕЛЬНЫЕ ***не используются***

4.6.2 Электронные издания

ОСНОВНЫЕ

1. Платонов В.В. Программно-аппаратные средства защиты информации (2-е изд., стер.), М. Академия, 2014, https://academia-library.ru/catalogue/4831/105545/
2. Душкин А.В., Барсуков О.М., Кравцов Е.В., Славнов К.В. Программно-аппаратные средства обеспечения информационной безопасности: учеб. Пособие. – М.: Горячая линия – Телеком, 2016.- 248 с. https://znanium.com/bookread2.php?book=973806
3. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 1. Правовое обеспечение информационной безопасности: учеб. Пособие. – М.: МИЭТ, 2016. – 184 с. https://znanium.com/bookread2.php?book=536932
4. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2016. – 172 с. https://znanium.com/bookread2.php?book=536932

ДОПОЛНИТЕЛЬНЫЕ:

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
3. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

4. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

5. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».

6. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

7. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

8. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

9. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.

10. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.

11. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

12. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.

13. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.

14. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.

15. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

16. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.

17. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.

18. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.

19. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.

20. Приказ ФАПСИ при Президенте Российской Федерации от 13 июня 2001 г. № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

21. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».

22. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий

23. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий

24. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер

25. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети

26. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью

27. 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

28. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности

29. ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности

30. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"

31. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"

32. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

33. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.

34. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.

35. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.

36. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

37. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005.

38. ГОСТ Р 50543-93 Конструкции базовые несущие. Средства вычислительной техники. Требования по обеспечению защиты информации и электромагнитной совместимости методом экранирования. Госстандарт России, 1993.

39. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.

40. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном

исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.

41. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.

42. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013.

43. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.

44. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

45. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

46. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

47. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

48. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

49. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

50. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

в) программное обеспечение: специализированное программное обеспечение для проверки защищенности помещений от утечки информации по акустическому и виброакустическому каналам, специальных исследований средств вычислительной техники;

г) базы данных, информационно-справочные и поисковые системы: www.fstec.ru; www.gost.ru/wps/portal/tk362.

4.6.3 Периодические издания:

1. Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей;
2. Защита информации. Инсайд: Информационно-методический журнал
3. Информационная безопасность регионов: Научно-практический журнал
4. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности.. URL: http://cyberrus.com/
5. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: http://bit.mephi.ru/

4.6.4 Электронные ресурсы:

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru

2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru

3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/

4. Справочно-правовая система «Консультант Плюс» www.consultant.ru

5. Справочно-правовая система «Гарант» » www.garant.ru

6. Федеральный портал «Российское образование www.edu.ru

7. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/

8. Российский биометрический портал www.biometrics.ru

9. Федеральный портал «Информационно- коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru

10. Сайт Научной электронной библиотеки www.elibrary.ru

4.6.5 Профессиональные базы данных и справочные системы

- Федеральная служба государственной статистики - https://rosstat.gov.ru/
- Наукометрическая и реферативная база данных SCOPUS - https://www.scopus.com
- Информационно-справочная система "КонсультантПлюс"

ПМ.03

4.6.1 Печатные издания

ОСНОВНЫЕ ***не используются***

ДОПОЛНИТЕЛЬНЫЕ ***не используются***

4.6.2 Электронные издания

1. Зайцев А.П., Мещеряков Р.В., Шелупанов А.А. Технические средства и методы защиты информации. 7-е изд., испр. 2017. http://znanium.com/catalog/product/560580

2. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2016. – 172 с. https://znanium.com/catalog/product/536932

3. Белов Е.Б. Организационно-правовое обеспечение информационной безопасности (1-е изд.), М. Академия, 2017 https://academia-library.ru/catalogue/4831/293834/

4.6.3 Дополнительные источники:

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

3. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

4. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

5. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».

6. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

7. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

8. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

9. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.

10. Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.

11. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.

12. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

13. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.

14. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.

15. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.

16. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

17. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.

18. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.

19. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.

20. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.

21. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».

22. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий

23. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий

24. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер

25. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети

26. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью

27. 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

28. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности

29. ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности

30. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"

31. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"

32. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

33. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.

34. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.

35. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.

36. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

37. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005.

38. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.

39. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.

40. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.

41. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013.

42. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России, 1995.

43. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.

44. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

45. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

46. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

47. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

48. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

49. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

50. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

в) программное обеспечение: специализированное программное обеспечение для проверки защищенности помещений от утечки информации по акустическому и виброакустическому каналам, специальных исследований средств вычислительной техники;

г) базы данных, информационно-справочные и поисковые системы: www.fstec.ru; www.gost.ru/wps/portal/tk362.

4.6.4 Электронные ресурсы:

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
4. Справочно-правовая система «Консультант Плюс» www.consultant.ru
5. Справочно-правовая система «Гарант» » www.garant.ru
6. Федеральный портал «Российское образование www.edu.ru
7. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/
8. Федеральный портал «Информационно-коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru
9. Сайт Научной электронной библиотеки www.elibrary.ru

4.6.5 Профессиональные базы данных и справочные системы

- Федеральная служба государственной статистики - https://rosstat.gov.ru/
- Наукометрическая и реферативная база данных SCOPUS - https://www.scopus.com
- Информационно-справочная система "КонсультантПлюс"

ПМ.04:

4.6.1 Печатные издания

ОСНОВНЫЕ ***не используются***

ДОПОЛНИТЕЛЬНЫЕ ***не используются***

4.6.2 Электронные издания

ОСНОВНЫЕ

1. Струмпэ Н.В. Оператор ЭВМ: Практические работы (9-е изд.), М. Академия, 2018, https://academia-library.ru/catalogue/4831/373424/

ДОПОЛНИТЕЛЬНЫЕ:

4.6.3 Электронные ресурсы

1. Информационный портал по безопасности www.SecurityLab.ru.
2. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
3. Сайт Научной электронной библиотеки www.elibrary.ru
4. Справочно-правовая система «Гарант» » www.garant.ru
5. Справочно-правовая система «Консультант Плюс» www.consultant.ru
6. Федеральный портал «Информационно-коммуникационные технологии в образовании» http:\\www.ict.edu.ru
7. Федеральный портал «Российское образование www.edu.ru

4.6.4 Профессиональные базы данных и справочные системы

- Федеральная служба государственной статистики - https://rosstat.gov.ru/
- Наукометрическая и реферативная база данных SCOPUS - https://www.scopus.com
- Информационно-справочная система "КонсультантПлюс"

Приложение № 1

Министерство науки и высшего образования Российской Федерации
федеральное государственное бюджетное образовательное учреждение высшего образования
«Российский экономический университет имени Г.В. Плеханова»
Московский приборостроительный техникум

УТВЕРЖДАЮ
Зам. директора по УР

_____ Д.А. Клопов
«__»_____20___года

ЗАДАНИЕ

на выпускную квалификационную работу (дипломный проект / дипломную работу) по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

студенту(ке)_____ группы _____
(фамилия, имя, отчество)

Разработать дипломный проект (дипломную работу) на тему: _____
_____
_____
_____

Содержание выпускной квалификационной работы
Введение

1. Общие положения
_____
_____
_____
_____

2. Аналитическая часть _____
_____
_____
_____
_____
_____

3. Проектная часть
_____
_____
_____
_____
_____
_____

4. Экспериментальная часть (если предусмотрено)
_____
_____
_____
_____
_____
_____

5. Техника безопасности или охрана труда
_____
_____

6. Графическая часть

График выполнения работы

№ п/п	Наименование работы	Срок выполнения

Дата выдачи «____»_____ 20___ года
Срок окончания «____»_____ 20___ года

Председатель цикловой методической комиссии
«Профессиональных модулей 10.02.05» _____ / _____ /
(подпись)
Заведующий отделением _____ / _____ /
(подпись)
Руководитель ВКР _____ / _____ /
(подпись)
Консультант (если назначен) _____ / _____ /
(подпись)
Студент _____ / _____ /
(подпись)