МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
Факультет информационных систем и безопасности
Кафедра информационной безопасности

ПРОГРАММА ПРАКТИКИ

Производственная
Преддипломная практика

по направлению подготовки 10.03.01 Информационная безопасность
Профиль: Организация и технология защиты информации (по отрасли или в сфере профессиональной деятельности)
Уровень квалификации выпускника (*бакалавр*)
Форма обучения (*очная*)

Программа практики адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва *2021*

Производственная
Преддипломная практика
Составитель:
к.и.н., доцент, заведующая кафедрой
информационной безопасности Г.А. Шевцова

УТВЕРЖДЕНО
Протокол заседания кафедры информационной безопасности
№ 10 от 20.05.2021 г.

ОГЛАВЛЕНИЕ

1. Пояснительная записка

Производственная преддипломная практика (Пд) является одним из разделов составляющей образовательной программы (ОП) и формирует у студентов компетенции в сфере профессиональной деятельности.

Производственная преддипломная практика составлена в соответствии с требованиями ФГОС ВО - Бакалавриат по направлению подготовки 10.03.01 Информационная безопасность от 17 ноября 2020 г. N 1427, Положением о практической подготовки обучающихся, утвержденным приказом Минобрнауки России от 05.08.2020 №885/390, Положением о практической подготовке обучающихся ФГБОУ ВО «Российский государственный гуманитарный университет», утв. приказом РГГУ от 03 ноября 2020 года № 01-568/осн и представляет особый вид учебных занятий, непосредственно ориентированных на профессионально - практическую подготовку обучающихся по получению профессиональных умений и опыта профессиональной деятельности.

Преддипломная практика реализуется на ФИСБ кафедрами «Информационной безопасности» и «Комплексная защита информации».

Цель производственной преддипломной практики: Преддипломная практика направлена на расширение и углубление теоретических знаний, формирование умений и навыков выполнения разработки и проектирования в профессиональной сфере, подготовки технических отчетных документов, окончательную формулировку темы и содержания выпускной квалификационной работы (ВКР). Состоит в формировании заданных универсальных, общепрофессиональных, общепрофессиональных компетенций, соответствующие выбранной направленности программы бакалавриата по профилю "Организация и технологии защиты информации" и профессиональных компетенций, обеспечивающих подготовку студентов к практической реализации эксплуатационных, организационно-управленческих, проектно-технологических и экспериментально-исследовательских работ в области обеспечения информационных и коммуникационных технологий (в сфере техники и технологии, охватывающих совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере).

Преддипломная практика проводится для выполнения выпускной квалификационной работы и является обязательной.

Задачи производственной преддипломной практики:

- выполнение этапов работы, определенных индивидуальным заданием, календарным планом, формой представления отчетных материалов и обеспечивающих выполнение планируемых в компетентностном формате результатов;

- окончательное формулирование темы, содержания и перечня материалов, в том числе графических, выпускной квалификационной работы;

- оформление отчета, содержащего материалы этапов и раскрывающего уровень освоения заданного перечня компетенций;

- подготовка и проведение защиты полученных результатов.

1.2. Вид (тип) практики – производственная преддипломная практика

1.3. Способы, формы и места проведения практики

Способы проведения практики: стационарная, выездная.

Стационарная практика проводится в структурных подразделениях РГГУ или в профильных организациях, расположенных на территории г. Москвы и Московской области.

Выездная практика проводится в профильных организациях различных регионов Российской Федерации.

Формы проведения практики: *дискретная (*путем выделения в календарном учебном графике непрерывного периода учебного времени для проведения каждого вида (совокупности видов) практик).

Места проведения практики.

№ п/п	Наименование юридического лица	№ договора, дата	Адрес проведения практики
1	Министерство науки и высшего образования Российской Федерации («Минобрнауки России»	№ 195-05-824/ФУ от 10.04.2019г., доп. Согл. № 1 от 11.06.2019 г.	г. Москва, ул. Тверская, д.11, стр.1, 4
2	Федеральное государственное бюджетное учреждение науки Институт проблем управления им. В.А. Трапезникова Российской академии наук (ИПУ РАН)	№ 195-05-78/ФИСБ от 03.06.2019 г.	г. Москва, ул. Профсоюзная, д.65
3	ФГУП «НПП Гамма»	№ 195-05-60а/ФИСБ от 27.12.2018 г.	г. Москва, ул. Профсоюзная, д.78 стр.4
4	Общество с ограниченной ответственностью «ЗАЩИТНЫЕ ТЕХНОЛОГИИ»	№ 195-05-74/ФИСБ от 29.04.2019 г.	г. Москва, ул. Харьковский проезд, д.2, стр.3
5	Общество с ограниченной ответственностью «Ангара Технолоджиз Груп»	№ 195-05-61/ФИСБ от 28.02.2019 г. Дополнительное соглашение № 1	г. Москва, ул. Василисы Кожиной, д.1

		от «12» февраля 2020 года	
6	Общество с ограниченной ответственностью «Лаборатория инноваций»	№ 195-05-77/ФИСБ от 03.06.2019 г.	г. Москва, ул.Тверская-Ямская 4-я, д.24
7	Акционерное общество коммерческий банк «ЮНИСТРИМ»	№ 195-05-75а/ФИСБ от 31.05.2019 г.	г. Москва, ул. Верхняя Масловка, д.20, стр.2
8	Общество с ограниченной ответственностью «Патентно-правовое бюро «Эксперт»	Договор № 12 от 16.06.2020 г.	г.Москва, Большая Серпуховская, д.44, оф.412
9	ИИНТБ РГГУ (лаборатория компьютерной техники и средств защиты информации)		г. Москва, ул. Кировоградская д.25 корп.2

1.4. Вид (виды) профессиональной деятельности
эксплуатационная деятельность:

установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;

администрирование подсистем информационной безопасности объекта;

участие в проведении аттестации объектов информатизации по требованиям безопасности информации и аудите информационной безопасности автоматизированных систем;

проектно-технологическая деятельность:

сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;

проведение проектных расчетов элементов систем обеспечения информационной безопасности;

участие в разработке технологической и эксплуатационной документации;

проведение предварительного технико-экономического обоснования проектных расчетов;

экспериментально-исследовательская деятельность:

сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования;

проведение экспериментов по заданной методике, обработка и анализ их результатов;

проведение вычислительных экспериментов с использованием стандартных программных средств;

организационно-управленческая деятельность:

осуществление организационно-правового обеспечения информационной безопасности объекта защиты;

организация работы малых коллективов исполнителей;

участие в совершенствовании системы управления информационной безопасностью;

изучение и обобщение опыта работы других учреждений, организаций и предприятий в области защиты информации, в том числе информации ограниченного доступа;

контроль эффективности реализации политики информационной безопасности объекта защиты.

При разработке и реализации программы бакалавриата РГГУ ориентируется на все виды профессиональной деятельности, к которым готовится бакалавр.

1.5 Планируемые результаты обучения при прохождении практики, соотнесённые с индикаторами достижения компетенций:

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	ОПК-12.1. Знает принципы формирования политики информационной безопасности в информационных системах; основные этапы процесса проектирования и общие требования к содержанию проекта ОПК-12.2. Умеет определять информационную инфраструктуру и информационные ресурсы организации, подлежащих защите; анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации ОПК-1.3. Владеет навыками по разработке основных показателей технико-экономического обоснования соответствующих проектных решений	*Знать:* назначение и основные технические характеристики информационных систем, их взаимосвязь с техническими средствами охраны и видеонаблюдения; основные руководящие, методические и нормативные документы по организационно-технической защите информации *Уметь:* описывать объекты защиты; выявлять источники угроз безопасности ресурсам организации; оценивать возможную величину ущерба от реализации угроз; *Владеть:* методикой по разработке организационно-методических и технических решений по обеспечению безопасности объекта защиты
ОПК-2.1 Способен	ОПК-2.1.1. Умеет анализировать угрозы	*Знать:* терминологию процессов и систем защиты

проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба	безопасности информации, оценивать информационные риски; применять аналитические и компьютерные модели автоматизированных систем и систем защиты информации; анализировать программные и программно-аппаратные решения при проектировании системы защиты информации с целью выявления уязвимостей ОПК-2.1.2. Умеет разрабатывать предложения по совершенствованию системы управления защиты информации, осуществлять планирование и организацию работы персонала с учетом требований по защите информации ОПК-2.1.3. Владеет навыками выработки рекомендаций для решения о модернизации системы защиты информации	информации; основные методы моделирования процессов и систем защиты информации, основные принципы и приемы построения моделей; основные нормативно-правовые акты, регламентирующие вопросы определения и моделирования угроз безопасности информации в информационных системах; методологии и средства процессов и систем. *Уметь:* использовать нормативно-правовые акты, регламентирующие вопросы определения угроз безопасности информации в информационных системах; использовать принципы и методы процессов и систем защиты информации; формулировать предложения по оптимизации и улучшению функционирования системы или процесса. *Владеть:* терминологией в области процессов и систем защиты информации; навыками использования правовых и нормативных требований к определению угроз безопасности информации в информационных системах; формулирования предложений по оптимизации и улучшению функционирования системы или процесса.
ОПК-2.2 Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных	ОПК-2.2.1 Знает организационные меры по защите информации, основные методы управления защитой информации ОПК-2.2.2 Умеет разрабатывать предложения по совершенствованию системы управления защиты	*Знать:* основные технические характеристики информационных систем; основные направления политики предприятий в области обеспечения комплексной безопасности; особенности организационно-правового

составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы	информации, осуществлять планирование и организацию работы персонала с учетом требований по защите информации ОПК-2.2.3 Владеет навыками выработки рекомендаций для решения о модернизации системы защиты информации	регулирования в области обеспечения комплексной безопасности. *Уметь:* оценивать возможную величину ущерба от реализации угроз; *Владеть:* методикой по разработке технических решений по обеспечению безопасности объекта защиты; классификацией защищаемой информации по видам тайны; навыками подбора, изучения и обобщения научно-технической литературы, нормативных материалов по вопросам обеспечения информационной безопасности.
ОПК-2.3. Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности	ОПК-2.3.1 Знает национальные, межгосударственные и международные стандарты в области защиты информации, нормативные правовые акты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти в области внедрения и эксплуатации средств защиты информации ОПК-2.3.2 Умеет документировать процедуры и результаты контроля функционирования системы защиты информации; проводить испытания программно-технических средств защиты информации от НСД и специальных воздействий на соответствие требованиям по безопасности информации и техническим условиям ОПК-2.3.3 Владеет навыками внесения изменений в эксплуатационную документацию и организационно-	*Знать:* закономерности развития предприятий различного типа и организацию их функционирования с целью достижения максимальной эффективности при минимальных затратах ресурсов; виды и особенности рисков, порождаемых системами документооборота; методы использования средств защиты информации при построении систем документооборота; методы обеспечения юридической силы электронных данных; основы действующего законодательства в области электронного документооборота *Уметь:* оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов; оценивать используемые системы документооборота с точки зрения обеспечения защищенности

	распорядительные документы по системе защиты информации; навыками разработки программ и методик испытаний опытного образца программно-технического средства защиты информации от НСД и специальных воздействий на соответствие техническим условиям	обрабатываемой информации и юридической силы электронных данных. *Владеть:* навыками использовать основы правовых знаний в различных сферах деятельности; основной терминологией, методами и основными алгоритмами реализации процесса
ОПК-2.4 Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами	ОПК-2.4.1 Знает критерии оценки защищенности объекта информатизации, технические средства контроля эффективности мер защиты информации, методы измерений, контроля и технических расчетом характеристик программно-аппаратных средств защиты информации ОПК-2.4.2 Умеет осуществлять контроль обеспечения уровня защищенности объектов информатизации ОПК-2.4.3 Владеет навыками оценки защищенности объектов информатизации с помощью типовых программных средств	*Знать:* место и роль информационной безопасности в системе; принципы построения системы управления информационной безопасностью в организации; процессный подход к организации информационной безопасности; нормативно-правовые и методологические основы информационной безопасности *Уметь:* использовать нормативно-правовые акты по ИБ; оценивать эффективность процессов управления ИБ организации; оценивать эффективность СУИБ организации; анализировать и оценивать текущее состояние ИБ на предприятии; исследовать полученные оценки информационной безопасности; оценивать результаты и самооценки информационной безопасности. *Владеть:* терминологией и процессным подходом к построению СУИБ; навыками анализа активов организации, угроз ИБ и уязвимостей в рамках области деятельности СУИБ; методами научного исследования уязвимости и

		защищенности информационных процессов; навыками использования методологии, правовых и нормативных требований и рекомендаций в области информационной безопасности.
Тип задач профессиональной деятельности: проектно-технологический		
ПК-7 Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	ПК-7.1 Знает разработку концепции средств и систем информатизации в защищенном исполнении, разработку технического задания на средство и/или систему информатизации в защищенном исполнении ПК-7.2 Умеет разрабатывать конструкторскую и технологическую документацию на средство и/или систему информатизации в защищенном исполнении ПК-7.3 Владеет навыками разработки рабочей и эксплуатационной документации на средства и системы информатизации в защищенном исполнении	*Знать:* порядок проектирования подсистем и средств обеспечения информационной безопасности. *Уметь:* проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности. *Владеть:* навыками участия в проведении технико-экономического обоснования проектных решений.
ПК-8 Способен оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	ПК-8.1 Знает нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа, проектирования средств защиты информации, сертификации средств защиты информации на соответствие требованиям по безопасности информации и аттестации объектов информатизации на соответствие требованиям по защите информации, стандарты ЕСКД, ЕСТД и ЕСПД ПК-8.2 Умеет оформлять рабочую и эксплуатационную документацию на средства и системы информатизации в защищенном исполнении ПК-8.3 Владеет навыками разработки технического	*Знать:* основные руководящие, методические и нормативные документы по организационно-технической защите информации *Уметь:* описывать объекты защиты; выявлять источники угроз безопасности ресурсам организации; оценивать возможную величину ущерба от реализации угроз; *Владеть:* методикой по разработке нормативных документов, технических решений по обеспечению безопасности объекта защиты

	проекта средства и/или системы информатизации в защищенном исполнении	
Тип задач проф. деятельности: экспериментально-исследовательский		
ПК-9 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	ПК-9.1 Знает нормативные правовые акты в области защиты информации, национальные, межгосударственные и международные стандарты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ПК-9.2 Владеет организационными мерами по защите информации ПК-9.3 Умеет работать с программным обеспечением с соблюдением действующих требований по защите информации	*Знать:* основную научно-технической литературу, нормативные и методические документы в области обеспечения информационной безопасности *Уметь:* оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов *Владеть:* навыками использовать основы правовых знаний в различных сферах деятельности
ПК-10 Способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	ПК-10.1 Знает нормативные правовые акты в области защиты информации, национальные, межгосударственные и международные стандарты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ПК-10.2 Умеет анализировать данные о назначении, функциях, условиях функционирования объектов и систем обработки информации ограниченного доступа, установленных на объектах информатизации, и характере обрабатываемой на них информации ПК-10.3 Владеет навыком разработки аналитического обоснования необходимости создания системы защиты информации в организации	*Знать:* основные нормативные правовые акты в области защиты информации *Уметь:* организовать согласование и утверждение документации по выполняемым работам с учетом требований нормативных документов в области информационной безопасности *Владеть:* навыками по разработки аналитического обоснования необходимости создания системы защиты информации в организации с учетом требований нормативных документов в области информационной безопасности
ПК-11 Способен проводить эксперименты по заданной методике, обработку, оценку	ПК-11.1 Знает методики проведения теоретических исследований уровней защищенности информационной	*Знать:* назначение и основные технические характеристики информационных систем, их

погрешности и достоверности их результатов	безопасности объектов и систем ПК-11.2 Умеет составлять и оформлять аналитический отчет по проведенным испытаниям, делать выводы по оценке защищенности на основании аналитического отчета ПК-11.3 Владеет навыками использования профиля защиты и задания по безопасности, формулирования выводов по оценке защищенности	взаимосвязь с техническими средствами охраны и видеонаблюдения; основные руководящие, методические и нормативные документы по организационно-технической защите информации *Уметь:* описывать объекты защиты; выявлять источники угроз безопасности ресурсам организации; оценивать возможную величину ущерба от реализации угроз *Владеть:* методикой по разработке технических решений по обеспечению безопасности объекта защиты
ПК-12 Способен принимать участие в проведении экспериментальных исследований системы защиты информации	ПК-12.1 Знает методы и технологии проектирования, моделирования, исследования систем защиты информации ПК-12.2 Умеет выполнять сбор, обработку, анализ и систематизацию информации в области защиты информации ПК-12.3 Владеет навыками по разработке и исследованию конкретных явлений и процессов для решения расчетных и исследовательских задач	*Знать:* методику проведения экспериментальных исследований системы защиты информации. *Уметь:* тестировать средства защиты информации автоматизированной системы от несанкционированного доступа на соответствие установленным правилам разграничения доступа. *Владеть:* навыками тестирования средств защиты информации автоматизированной системы от несанкционированного доступа
Тип задач профессиональной деятельности: организационно-управленческий		
ПК-13 Способен принимать участие в формировании, организации и поддержания выполнения комплекса мер по обеспечению информационной безопасности, управлении процессом	ПК-13.1 Знает процедуру организации установки и настройки технических, программных (программно-технических) средств защиты информации, входящих в состав системы защиты информации организации, в соответствии с техническим проектом и инструкциями по эксплуатации	*Знать:* структуру, задачи и функции системы обеспечения информационной безопасности организаций; особенности правового регулирования деятельности по организации защиты информации в организациях; состав угроз

их реализации	ПК-13.2 Умеет разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы защиты информации ПК-13.3 Владеет навыками организации и сопровождения аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации	защищаемой информации в организациях и методику их выявления, методику анализа и оценки рисков нарушения информационной безопасности организаций, основы менеджмента рисков нарушения информационной безопасности *Уметь:* разрабатывать требования по обеспечению информационной безопасности организаций и внедрять меры по их обеспечению; проводить анализ эффективности защиты с точки зрения ее соответствия требованиям действующих нормативных документов и лучшим практикам. *Владеть:* навыками разработки требований к системе обеспечения информационной безопасности в организациях на основе действующих отраслевых стандартов; навыками эффективного внедрения мер по защите информации в существующие технологические процессы обработки информации в информационных системах организаций
ПК-14 Способен организовывать работу малого коллектива исполнителей в профессиональной деятельности	ПК-14.1 Знает организацию проведения инструктажа руководящего состава и обучения персонала по вопросам защиты информации ПК-14.2 Умеет организовать работу персонала по использованию технических, программных (программно-технических) средств защиты информации ПК-14.3 Владеет навыками по осуществлению планирования и организации работы персонала с	*Знать:* роль и место управления персоналом в организационном управлении и его связь со стратегическими задачами организации, работающей в области ИБ; причины многовариантности практики управления персоналом в современных условиях; бизнес-процессы в сфере управления персоналом и роль в них линейных

	учетом требований по защите информации	менеджеров и специалистов по управлению персоналом. *Уметь:* проводить аудит человеческих ресурсов организации, работающей в области ИБ, прогнозировать и определять потребность организации в персонале, определять эффективные пути ее удовлетворения; разрабатывать мероприятия по привлечению и отбору новых сотрудников и программы их адаптации; разрабатывать программы обучения сотрудников и оценивать их эффективность; использовать различные методы оценки и аттестации сотрудников и участвовать в их реализации; разрабатывать мероприятия по мотивированию и стимулированию персонала организации. *Владеть:* навыками организации работы малого коллектива исполнителей; навыками исследования системы управления персоналом; навыками анализа качественных и количественных данных; навыками выявления ключевых проблем в области управления персоналом.
ПК-15 Способен организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной	ПК-15.1 Знает технологический процесс защиты информации и процедуру разработки технических заданий, планов и графиков проведения работ по защите информации в соответствии с действующим нормативными и методическими документами ПК-15.2 Умеет применять национальные, межгосударственные и международные стандарты в области защиты информации,	*Знать:* особенности правового регулирования деятельности по организации защиты информации в организациях; состав угроз защищаемой информации в организациях и методику их выявления, методику анализа и оценки рисков нарушения информационной безопасности организаций, основы менеджмента рисков

службы по техническому и экспортному контролю	применять действующую законодательную базу в области обеспечения защиты информации, читать и понимать нормативные и методические документы по информационной безопасности на английском языке ПК-15.3 Владеет навыками по контролю над соблюдением установленного порядка выполнения работ, а также действующего законодательства Российской Федерации при решении вопросов, касающихся защиты информации	нарушения информационной безопасности; требования к системе защиты информации учреждений и предприятий и методы оценки их соблюдения. *Уметь:* проводить анализ эффективности защиты с точки зрения ее соответствия требованиям действующих нормативных документов и лучшим практикам. *Владеть:* навыками эффективного внедрения мер по защите информации в существующие технологические процессы обработки информации в информационных системах организаций; навыками выработки рекомендаций по составу организационно-технических мер по защите информации в организациях, направленных на повышение защищенности их информационных; методикой оценки соответствия действующей в организации системы обеспечения информационной безопасности требованиям отраслевых стандартов.

1.6. Место практики в структуре образовательной программы

Производственная преддипломная практика относится к блоку Б2 («Практики») учебного плана, реализуемая в 8-ом учебном семестре, выполняет интегрирующие функции в формировании навыков (владений) самостоятельного применения изученных в рамках профессиональных и профильных дисциплин инструментов и методов разработки, проектирования, моделирования и организационно-управленческих в предметной области.

Прохождение производственной преддипломной практики способствует формированию навыков (владений) самостоятельного применения изученных в рамках

профессиональных и профильных дисциплин, базируется на изученных дисциплинах учебного плана по направлению подготовки «Информационная безопасность».

Производственная преддипломная практика обеспечивает возможность подойти с углубленным пониманием по теоретической подготовки и с приобретенными практическими навыками и компетенциями к написанию ВКР.

Производственная преддипломная практика является разделом деятельностной части образовательной программы подготовки бакалавров. Выполнение Преддипломной практики направлено, прежде всего, на формирование деятельностных компонентов компетенции («уметь», «владеть»). Компонента «знать» при выполнении Преддипломной практики, как правило, актуализируется содержанием задач разработки и проектирования в области информационной безопасности и защиты информации. Важно, что продолжительность выполнения Преддипломной практики, комплексный характер тематики и наличие этапа практического применения результатов позволяют обеспечить формирование компоненты «владеть» компетенций, закрепленных за Преддипломной практикой. Преддипломная практика по своей тематике ориентирована на решение задач проектирования и внедрения решений в области информационной безопасности и защиты информации. Преддипломная практика выполняет интегрирующую роль, объединяя выполнение различных форм самостоятельной работы бакалавра. Результаты выполнения Преддипломной практики, как правило, составляют основу для практико-ориентированных разделов выпускной квалификационной работы бакалавра.

1.7. Объем практики

Преддипломная практика рассчитана на 6 недель 342 часа, 9 з.е., проводится в 8 семестре, в том числе контактная работа 36 часов, самостоятельная работа 306 часов, в соответствии с учебным планом и календарным графиком.

2. Содержание практики

Производственная преддипломная практика выполняется по тематике, связанной с основным направлением исследований и имеет целью подготовку материала для выполнения проектного и внедренческого разделов выпускной квалификационной работы бакалавра.

Согласно ФГОС ВО - Бакалавриат по направлению подготовки 10.03.01 Информационная безопасность от 17 ноября 2020 г. N 1427, содержание Преддипломной практики должно предусматривать участие в выполнении работ по следующим направлениям:

№	Наименование раздела	Содержание и виды работ
1	Компонент системы обеспечения информационной	установка, настройка, эксплуатация и поддержание

	безопасности	в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований
2	Аттестация объекта	участие в проведении аттестации объектов, помещений, технических средств, систем, программ и алгоритмов на предмет соответствия требованиям защиты информации
3	Администрирование подсистем информационной безопасности объекта	администрирование подсистем информационной безопасности объекта; - сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования;
4	Экспериментальная обработка	- проведение экспериментов по заданной методике, обработка и анализ результатов;
5	Вычислительные эксперименты	- проведение вычислительных экспериментов с использованием стандартных программных средств.
6	Промежуточный контроль	Подготовка и защита отчёта по практике
	Итог:	Зачет с оценкой

Местом прохождения производственной преддипломной практики являются подразделения предприятий и организаций, специализирующихся в области обеспечения информационной безопасности и защиты информации.

Производственная преддипломная практика полностью ориентирована на самостоятельную работу. Консультации и текущий контроль выполнения этапов практики осуществляет руководитель по месту практики во время запланированных консультаций.

3. Оценка результатов практики - *проверка сформированности следующих компетенций ОПК-12; ОПК-2.1; ОПК-2.2; ОПК-2.3; ОПК-2.4; ПК-7; ПК-8; ПК-9; ПК-10; ПК-11; ПК-12; ПК-13; ПК-14; ПК-15*

3.1. Формы отчётности

По окончании практики каждый студент составляет отчет, который включает следующие разделы: введение, организация работы по разделам программы и заключение, включая предложения и замечания. Отчет составляется в рабочей тетради или на листах формата А4. Титульный лист отчета должен отвечать требованиям, предъявляемым к титульным листам курсовых работ. В основу отчета берутся записи в дневнике, где фиксируются задания, объем выполненной работы, вопросы, требующие разрешения и т.д. Дневниковые записи ведутся в произвольной форме в рабочей тетради.

Работа каждого студента оценивается совместно руководителем практики и выделенным преподавателем от кафедры «Информационной безопасности» на основании представленного отчета. Итоги практики подводятся на собрании студентов после ее окончания.

Тематика преддипломной практики определяется направлениями научных исследований в области разработки, проектирования и внедрения в области информационной безопасности и защиты информации. Темы Пд должны соответствовать определенным требованиям:

1. Относиться к актуальным направлениям развития науки и техники и приоритетному направлению развития.

2. Соответствовать содержанию основных разделов профильных дисциплин и тематике выпускных квалификационных работ бакалавров.

3. Соответствовать одному из научных направлений профильной или выпускающей кафедр.

4. Быть коррелированными с тематикой НИР.

5. Иметь практическую целесообразность и инновационную направленность.

6. Обуславливать творческий характер задач проектирования и конструирования.

7. Обеспечить наличие элементов внедрения.

8. Использовать современные информационные технологии.

Темы преддипломной практики должны обеспечивать следующие свойства выполняемой в рамках практики работе:

- актуальность;
- практикоориентированность;
- инновационность;
- наличие этапов проектирования и оценивания эффективности решений;
- наличие элементов внедрения.

Темы Производственной преддипломной практики разрабатываются руководителем по месту практики и согласовываются с руководителем практики от университета и заведующим выпускающей кафедрой.

3.2.Критерии выставления оценки по практике

Баллы/ Шкала ECTS	**Оценка по практике**	**Критерии оценки результатов практики**
100-83/ A,B	*«отлично»/ «зачтено (отлично)»/ «зачтено»*	Выставляется обучающемуся, если характеристика с места прохождения практики содержит высокую положительную оценку, отчет выполнен в полном соответствии с предъявляемыми требованиями, аналитическая часть отчета отличается комплексным подходом, креативностью и нестандартностью мышления студента, выводы обоснованы и подкреплены значительным объемом фактического материала. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Компетенции, закреплённые за практикой, сформированы на уровне – «высокий».
82-68/ C	*«хорошо»/ «зачтено (хорошо)»/ «зачтено»*	Выставляется обучающемуся, если характеристика с места прохождения практики содержит положительную оценку, отчет выполнен в целом в соответствии с предъявляемыми требованиями без существенных неточностей, включает фактический материал, собранный во время прохождения практики.. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D,E	*«удовлетвори-тельно»/ «зачтено (удовлетвори-тельно)»/ «зачтено»*	Выставляется обучающемуся, если характеристика с места прохождения практики содержит положительную оценку, отчет по оформлению и содержанию частично соответствует существующим требованиями, но содержит неточности и отдельные фактические ошибки, отсутствует иллюстративный материал. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	*«неудовлетворительно»/ не зачтено*	Выставляется обучающемуся, если характеристика с места прохождения практики не содержит положительной оценки. Отчет представлен не вовремя и не соответствует существующим требованиям.

Баллы/ Шкала ECTS	Оценка по практике	Критерии оценки результатов практики
		Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

3.3. Оценочные средства (материалы) для промежуточной аттестации обучающихся по практике

Текущий контроль хода выполнения задания по практике проводится периодически (не реже 1 раза в неделю) в форме собеседования студента с руководителем по месту практики. На собеседованиях обсуждаются текущие вопросы, и контролируется качество выполнения составляющих самостоятельной работы: состояние выполняемого этапа проектно-конструкторских работ, результатов освоения инструментальной среды и т.д. Промежуточная аттестация выполнения задания по практике производится в форме защиты отчета. Отчет по практике является средством контроля. В отчете результаты освоения элементов закрепленных компетенций должны приводиться в компетентностном формате. Отчет защищается студентом перед комиссией, составленной распоряжением заведующего кафедрой из ведущих преподавателей (с участием руководителя практики от университета). В процессе защиты отчета у членов комиссии формируется мнение о соответствии представленных результатов заявленному уровню освоения элементов закрепленных компетенций. Процедура оценивания уровня освоения заданного перечня элементов компетенций должна проводиться на основе разработанных методических рекомендаций по формированию и применению контрольно-оценочных средств практики. Студенты, не выполнившие программу практики без уважительной причины или получившие неудовлетворительную оценку, могут быть отчислены как имеющие академическую задолженность в порядке, предусмотренном уставом вуза.

Для аттестации обучающихся на соответствие их учебных достижений требованиям ФГОС ВО в рамках выполнения Пд создается фонд оценочных средств Пд (ФОС Пд), являющийся составной частью системы оценки качества освоения образовательной программы. Фонд оценочных средств представляет собой комплект контрольно-оценочных и организационно-методических материалов, обеспечивающих оценку степени соответствия фактически достигнутого обучающимся уровня освоения заданных универсальных, общепрофессиональных, общепрофессиональных компетенций, соответствующие выбранной направленности программы бакалавриата по профилю

"Организация и технологии защиты информации" и профессиональных компетенций требованиям ФГОС ВО и ОП вуза. Результаты выполнения Пд как объекты контроля представляются обучающимися для контроля поэтапно в формах промежуточных и заключительного отчетов, содержащих результаты исследований по этапам. Объектами контроля (в компетентностном формате) являются компоненты контролируемых компетенций, представленные соответствующими индикаторами уровня освоения компонентов компетенций.

Индикаторы освоения компонентов компетенций - это описания объектов и/или действий над объектами компетенций, представленные в удобной для диагностирования форме. Индикаторы являются объектами оценивания степени соответствия достигнутого уровня освоения контролируемых компонентов компетенций требованиям ФГОС ВО. Как объекта оценивания, индикаторы представляют собой описание объекта деятельности компонента компетенции и/или производимые над ним действия, содержащееся в разделе отчета о Пд, или в ответе обучающегося в ходе защиты отчета о Пд. При этом индикаторы контролируемых и оцениваемых компонентов компетенций представляют собой инструменты решения профессиональных задач (методы, способы, модели, алгоритмы и пр.), а также механизмы применения этих инструментов (действия с инструментами). При высокой степени соответствия достигнутого обучающимися уровня освоения в ходе выполнения Пд компонентов компетенций требованиям ФГОС ВО следует вывод о том, что результаты обучения соответствуют требованиям ФГОС ВО.

В состав фонда оценочных Пд входят контрольно-оценочные материалы, предназначенные для контроля и оценивания уровней освоения заданных компетенций:

- агрегированная компетентностная модель (АКМ), используемая при контроле и оценивании уровней освоения заданных компетенций;
- общая спецификация контролируемых компетенций;
- критерий соответствия;
- шкала оценивания ;
- отчет о преддипломной практике
- отзыв руководителя Пд;
- индивидуальные задания на выполнение преддипломной практики обучающихся;
- процедура проведения защиты отчета о выполнении Пд.

Система текущего и промежуточного контроля прохождения преддипломной практики выстраивается в соответствии с учебным планом основной образовательной программы и предусматривает следующее распределение:

собеседование – 2 балла за каждый раздел отчета (этап) – максимально 10 баллов;

индивидуальные задания на выполнение преддипломной практики обучающихся – 55 баллов;

составление и защита отчета – до 35 баллов.

Итого: 100 баллов за преддипломную практику.

Фонд оценочных средств, представляет собой отдельный документ, находящийся на выпускающей кафедре.

4. Учебно-методическое и информационное обеспечение практики

4.1. Список источников и литературы

Источники

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/

Закон Российской Федерации от 21.07.93 № 5485-1 “О государственной тайне”, Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_2481/

Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_48699/

Федеральный закон от 28.12.2010 №390-ФЗ «О безопасности», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_108546/

Федеральный закон от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_113658/

Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/

Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_40241/

Указ Президента Российской Федерации от 06.03.97 № 188 “Об утверждении перечня сведений конфиденциального характера”, Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_13532/

Постановление Правительства Российской Федерации от 15.04.1995 № 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_6387/

Постановление Правительства Российской Федерации от 06.02.2010 № 63 «Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_97474/

Постановление Правительства Российской Федерации от 03.11.94 № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_54870/

ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности, дата введения 2011-12-01, Режим доступа: http://docs.cntd.ru/document/gost-r-iso-mek-27005-2010

Основная литература

Информационная безопасность предприятия : учеб. пособие / Н.В. Гришина. — 2-е изд., доп. — М. : ФОРУМ : ИНФРА-М, 2017. — 239 с. : ил. — (Высшее образование: Бакалавриат). - Режим доступа: http://znanium.com/catalog/product/612572

Ворона В.А., Тихонов В.А. Системы контроля и управления доступом. - М.: Горячая линия - Телеком, 2010. - 274 с. - Режим доступа: URL: http://znanium.com/catalog/product/560195 или https://docplayer.ru/25941028-V-a-vorona-v-a-tihonov-sistemy-kontrolya-i-upravleniya-dostupom.html

Груба И.И. Системы охранной сигнализации. Технические средства обнаружения. М.: СОЛОН-Пр., 2013. - 220 с. - Режим доступа: URL: http://znanium.com/catalog/product/883786

Ельчанинова, Н.Б. Правовые основы защиты информации с ограниченным доступом : учебное пособие / Н.Б. Ельчанинова ; Южный федеральный университет. - Ростов-на-Дону - Таганрог : Издательство Южного федерального университета, 2017. - 76 с. - ISBN 978-5-9275-2501-0. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1021578

Веселов, Г. Е. Менеджмент риска информационной безопасности: Учебное пособие / Веселов Г.Е., Абрамов Е.С., Шилов А.К. - Таганрог:Южный федеральный университет, 2016. - 107 с.: ISBN 978-5-9275-2327-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/997108

Золотарев, В. В. Управление информационной безопасностью. Ч. 1. Анализ информационных рисков [Электронный ресурс] : учеб. пособие/ В. В. Золотарев, Е. А.

Данилова. - Красноярск :Сиб. гос. аэрокосмич. ун-т, 2010. - 144 с. - Режим доступа: http://znanium.com/catalog/product/463037

Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2020. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/450371

Белов, П. Г. Системный анализ и программно-целевой менеджмент рисков : учебник и практикум для вузов / П. Г. Белов. — Москва : Издательство Юрайт, 2020. — 289 с. — (Высшее образование). — ISBN 978-5-534-04690-8. — Текст: электронный // ЭБС Юрайт — URL: https://urait.ru/bcode/454245

Дополнительная литература

Государственная тайна и ее защита в Российской Федерации : учеб. пособие для студентов вузов, обучающихся по направлению подгот. 220100 - "Систем. анализ и упр." / П. П. Аникин [и др.] ; под общ. ред.: М. А. Вуса и А. В. Федорова ; Ассоц. Юрид. центр, С.-Петерб. ин-т информатики и автоматизации РАН, Междунар. комис. по защите гос. тайны. - 3-е изд., испр. и доп. - СПб. : Юрид. центр Пресс, 2007. - 745 с. - (Государственное управление и государственный надзор и контроль).

Правовое обеспечение информационной безопасности : учеб. пособие для студентов вузов, обучающихся по специальностям: 075200 - Компьютерная безопасность, 075500 - Комплексное обеспечение информ. безопасности автоматизированных систем, 075600 - Информ. безопасность телекоммуникационных систем / [С. Я. Казанцев и др.] ; под ред. С. Я. Казанцева. - М. : Академия, 2005. - 238 с. - (Высшее профессиональное образование. Информационная безопасность).

Организационно-правовое обеспечение информационной безопасности : [учеб. пособие] / [А. А. Стрельцов и др.] ; под ред. А. А. Стрельцова. - М. : Академия, 2008. - 248 с. - (Высшее профессиональное образование. Информационная безопасность).

Правовое обеспечение информационной безопасности : учебник / [авт.-ред. В. А. Минаев и др.]. - Изд. 2-е, расшир. и доп. - М. : Маросейка, 2008. - 368 с. - (Серия "Информатика и информационная безопасность").

Романов О. А. Организационное обеспечение информационной безопасности : учебник для студентов вузов, обучающихся по специальностям "Орг. и технология

защиты информ." и "Комплекс. защита объектов информ." направления подгот. "Информ. безопасность" / О. А. Романов, С. А. Бабин, С. Г. Жданов. - М. : Академия, 2008. - 188 с. - (Высшее профессиональное образование. Информационная безопасность).

Управление персоналом организации: технологии управления развитием персонала: Учебник / Минева О.К., Ахунжанова И.Н., Мордасова Т.А.; Под ред. Миневой О.К. - М.:НИЦ ИНФРА-М, 2016. - 160 с.: 60x90 1/16. - (ВО: Бакалавр.) (О) ISBN 978-5-16-011743-0 - Режим доступа: http://znanium.com/catalog/product/542393

Концепция компетентностного подхода в управлении персоналом: Монография / Кибанов А.Я., Митрофанова Е.А., Коновалова В.Г. - Москва :НИЦ ИНФРА-М, 2017. - 156 с. (Научная мысль) (Обложка. КБС)ISBN 978-5-16-009530-1. - Текст : электронный. - URL: https://znanium.com/catalog/product/509288.

Информационная безопасность и защита информации : учеб. пособие / Баранова Е.К., Бабаш А.В. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2019. — 322 с. — (Высшее образование). — ww.dx.doi.org/10.12737/11380. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1009606

Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва: ИНФРА-М, 2020. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст: электронный. - URL: https://znanium.com/catalog/product/1018665

Захарова О.А., Селихина А.В., Везиров Т.Г. Моделирование информационно-аналитической системы мониторинга производственной безопасности на основе экспертных оценок // Вестник Донского государственного технического университета. 2020. Т. 20. № 1. С. 100-105. — Режим доступа: URL: https://elibrary.ru/download/elibrary_42684064_55636880.pdf

Карганов В.В. Основные положения по требованиям безопасности информации в части аттестации объектов информатизации. В сборнике: Национальная безопасность России: актуальные аспекты. Сборник избранных статей Всероссийской научно-практической конференции. Санкт-Петербург, 2020. С. 22-27. — Режим доступа: URL: https://elibrary.ru/download/elibrary_43114067_87155282.pdf

Информационные технологии в юридической деятельности : учебник для вузов / П. У. Кузнецов [и др.] ; под общей редакцией П. У. Кузнецова. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 325 с. — (Высшее образование). — ISBN 978-5-534-02598-9. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/449842

Белов, П. Г. Управление рисками, системный анализ и моделирование в 3 ч. Часть 1 : учебник и практикум для вузов / П. Г. Белов. — Москва : Издательство Юрайт, 2020. — 211 с. — (Высшее образование). — ISBN 978-5-534-02606-1. — Текст : электронный // ЭБС Юрайт — URL: https://urait.ru/bcode/451702

4.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

КонсультантПлюс [Электронный ресурс]. – Электрон. дан. – М. : КонсультантПлюс, – Режим доступа : www.consultant.ru.

4.3. Перечень БД и ИСС

№п/п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2020 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2020 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
3	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам Электронная библиотека Grebennikon.ru
4	Компьютерные справочные правовые системы Консультант Плюс, Гарант

5. Материально-техническая база, необходимая для проведения практики

Материально-техническая база включает учебные аудитории для групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Современный компьютерный класс оснащен

Состав программного обеспечения (ПО)

№п/п	Наименование ПО	Производитель	Способ распространения (*лицензионное или свободно распространяемое*)
1	Adobe Master Collection CS4	Adobe	лицензионное
2	Microsoft Office 2010	Microsoft	лицензионное
3	Windows 7 Pro	Microsoft	лицензионное
4	AutoCAD 2010 Student	Autodesk	свободно распространяемое
5	Archicad 21 Rus Student	Graphisoft	свободно

			распространяемое
6	SPSS Statisctics 22	IBM	лицензионное
7	Microsoft Share Point 2010	Microsoft	лицензионное
8	SPSS Statisctics 25	IBM	лицензионное
9	Microsoft Office 2013	Microsoft	лицензионное
10	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное
11	Microsoft Office 2013	Microsoft	лицензионное
12	Windows 10 Pro	Microsoft	лицензионное
13	Kaspersky Endpoint Security	Kaspersky	лицензионное
14	Microsoft Office 2016	Microsoft	лицензионное
15	Visual Studio 2019	Microsoft	лицензионное
16	Adobe Creative Cloud	Adobe	лицензионное
17	Zoom	Zoom	лицензионное

включающий наряду с компьютерами, подключёнными к сети Интернет, экран и проектор.

Материально-техническое обеспечение практики предоставляется принимающей организацией, имеющей необходимое лицензионное программное обеспечение, оборудование, демонстрационные приборы, специально оборудованные помещения и лаборатории.

В период временного приостановления посещения обучающимися помещений и территории РГГУ. для организации учебного процесса с применением электронного обучения и дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:

– видео-лекции;

– онлайн-лекции в режиме реального времени;

– электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;

– системы для электронного тестирования;

– консультации с использованием телекоммуникационных средств.

6. Организация практики для лиц с ограниченными возможностями здоровья

При необходимости программа практики может быть адаптирована для обеспечения образовательного процесса лицам с ограниченными возможностями здоровья, в том числе для дистанционного обучения. Для этого от студента требуется представить заключение психолого-медико-педагогической комиссии (ПМПК) и личное заявление (заявление законного представителя).

В заключении ПМПК должно быть прописано:

- рекомендуемая учебная нагрузка на обучающегося (количество дней в неделю, часов в день);

- оборудование технических условий (при необходимости);

- сопровождение и (или) присутствие родителей (законных представителей) во время учебного процесса (при необходимости);

- организация психолого-педагогического сопровождение обучающегося с указанием специалистов и допустимой нагрузки (количества часов в неделю).

Для осуществления процедур текущего контроля успеваемости и промежуточной аттестации обучающихся при необходимости могут быть созданы фонды оценочных средств, адаптированные для лиц с ограниченными возможностями здоровья и позволяющие оценить достижение ими запланированных в основной образовательной программе результатов обучения и уровень сформированности всех компетенций, заявленных в образовательной программе.

Форма проведения текущей и итоговой аттестации для лиц с ограниченными возможностями здоровья устанавливается с учетом индивидуальных психофизических особенностей (устно, письменно (на бумаге, на компьютере), в форме тестирования и т.п.). При необходимости студенту предоставляется дополнительное время для подготовки ответа на зачете или экзамене.

Форма проведения практики для обучающихся из числа лиц с ограниченными возможностями здоровья (инвалидностью) устанавливается с учетом индивидуальных психофизических особенностей в формах, адаптированных к ограничениям их здоровья и восприятия информации (устно, письменно на бумаге, письменно на компьютере и т.п.).

Выбор мест прохождения практик для инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) производится с учетом требований их доступности для данных обучающихся и рекомендации медико-социальной экспертизы, а также индивидуальной программе реабилитации инвалида, относительно рекомендованных условий и видов труда.

При направлении инвалида и обучающегося с ОВЗ в организацию или предприятие для прохождения предусмотренной учебным планом практики Университет согласовывает с организацией (предприятием) условия и виды труда с учетом рекомендаций медико-социальной экспертизы и индивидуальной программы реабилитации инвалида. При необходимости для прохождения практик могут создаваться специальные рабочие места в соответствии с характером нарушений, а также с учетом профессионального вида деятельности и характера труда, выполняемых обучающимся-инвалидом трудовых функций.

Защита отчета по практике для обучающихся из числа лиц с ограниченными возможностями здоровья осуществляется с использованием средств общего и специального назначения. Перечень используемого материально-технического обеспечения:

- учебные аудитории, оборудованные компьютерами с выходом в интернет, видеопроекционным оборудованием для презентаций, средствами звуковоспроизведения, экраном;
- библиотека, имеющая рабочие места для обучающихся, оборудованные доступом к базам данных и интернетом;
- компьютерные классы;
- аудитория Центра сопровождения обучающихся с инвалидностью с компьютером, оснащенная специализированным программным обеспечением для студентов с нарушениями зрения, устройствами для ввода и вывода голосовой информации.

Для лиц с нарушениями зрения материалы предоставляются:

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

Защита отчета по практике для лиц с нарушениями зрения проводится в устной форме без предоставления обучающихся презентации. На время защиты в аудитории должна быть обеспечена полная тишина, продолжительность защиты увеличивается до 1 часа (при необходимости). Гарантируется допуск в аудиторию, где проходит защита отчета, собаки-проводника при наличии документа, подтверждающего ее специальное обучение, выданного по форме и в порядке, утвержденных приказом Министерства труда и социальной защиты Российской Федерации 21 июля 2015г., регистрационный номер 38115).

Для лиц с нарушениями слуха защита проводится без предоставления устного доклада. Вопросы комиссии и ответы на них представляются в письменной форме. В случае необходимости, вуз обеспечивает предоставление услуг сурдопереводчика.

Для обучающихся с нарушениями опорно-двигательного аппарата защита итогов практики проводится в аудитории, оборудованной в соответствии с требованиями

доступности. Помещения, где могут находиться люди на креслах-колясках, должны размещаться на уровне доступного входа или предусматривать пандусы, подъемные платформы для людей с ограниченными возможностями или лифты. В аудитории должно быть предусмотрено место для размещения обучающегося на коляске.

Дополнительные требования к материально-технической базе, необходимой для представления отчета по практике лицом с ограниченными возможностями здоровья, обучающийся должен предоставить на кафедру не позднее, чем за два месяца до проведения процедуры защиты.

7. Этапы выполнения производственной преддипломной практики

7.1. Выполнение раздела ОП «Преддипломная практика» предусматривает:

- знакомство с профилем деятельности и организационной структурой предприятия (организации), а также структурного подразделения, в котором осуществляется практика;

- определение темы, содержания и перечня графических материалов выпускной квалификационной работы;

- содержание основных этапов выполнения экспериментально - исследовательских работ и проектных работ;

- перечень и характеристики планируемого к использованию современного инструментария проектирования, исследования и оценивания эффективности проектных решений;

- оформление результатов;

- подведение итогов выполнения Пд;

- разработку отчета и его защиту на заседании комиссии выпускающей кафедры.

7.2. Виды самостоятельной работы, выполняемой в процессе реализации преддипломной практики

Производственная преддипломная практика представляет собой самостоятельную учебную деятельность, выполняемую по индивидуальному заданию и под контролем руководителя практики. Основным видом самостоятельной работы в рамках Пд является выполнение составляющих проектных, конструкторских работ по этапам, обеспечивающих освоение заданных компетенций. По результатам выполнения практики студент должен подготовить отчет по Пд.

7.3. Основные требования к выполнению преддипломной практики

7.3.1. Требования к выполнению Пд

Основные требования к выполнению Пд:

- в ходе выполнения Пд должен быть освоен заданный перечень инструментов проектирования ИБиЗИ;

- должен быть предложен и обоснован комплексный критерий оценки проектных решений для подсистем ИБиЗИ;

- должна быть разработана методика сравнительного оценивания и выбора проектных решений подсистем ИБиЗИ и выполнена ее практическая реализация.

7.3.2. Требования к разрабатываемой отчетной документации Пд

В ходе выполнения Пд должен быть разработан, согласован и утвержден отчет по Пд, оформленный в соответствии с требованиями ГОСТ.

В отчете обязательно должна присутствовать информация, позволяющая дать оценку уровню освоения закрепленных частей компетенций. В отчете необходимо представить подробную информацию о руководителе ВКР от предприятия, тему, содержание и перечень графических материалов ВКР. Рекомендуемый объем отчета по практике 20-30 страниц (без учета приложений). К основному разделу отчета прикладываются индивидуальное задание, график выполнения Пд и характеристика руководителя по месту практики. Отчет подписывается студентом, проверяется руководителем по месту практики, руководителем практики от университета и утверждается заведующим кафедрой.

7.3.3. Требования к индивидуальному заданию на выполнение Пд

Индивидуальное задание является важным регламентирующим документом Пд, поскольку оно устанавливает объем, содержание и календарный план выполнения этапов. Индивидуальное задание на преддипломную практику составляется руководителем по месту практики, подписывается им, исполнителем, руководителем практики от университета и утверждается заведующим выпускающей кафедрой.

Индивидуальное задание на Пд должно содержать следующие разделы:

- полное наименование учебного заведения, факультета, кафедры, направления, профиля подготовки;

- наименование документа с указанием номера семестра;

- тема задания;

- срок сдачи отчета;

- содержание задания;

- календарный план выполнения, включающий наименование, содержание и сроки выполнения этапов;

- место выполнения Пд;

- подписи исполнителя, руководителя по месту практики и руководителя практики от университета.

В разделе «Содержание задания» должны быть указаны объекты контроля уровня освоения заданных компонентов компетенций: методики, методы, технологии проектирования, алгоритмы, инструментальные средства и т.д.

В методических указаниях студентам по выполнению Пд должны быть даны детальные разъяснения, касающиеся особенностей (полноты, глубины, обоснованности и т.д.) представления в отчетах объектов контроля, позволяющих проводить оценку уровня их освоения.

7.3.4. Требования к обеспечению Пд

Для выполнения преддипломной практики требуются следующие виды обеспечения:

- организационно-методическое;
- информационное;
- материально-техническое;
- кадровое.

Организационно-методическое обеспечение направлено на создание условий выполнения индивидуальных заданий по реализуемым видам Пд.

Организационно- методическое обеспечение Пд включает:

- Положение о практиках в РГГУ;
- Положение о самостоятельной работе студентов РГГУ;
- Методические указания студенту по выполнению задания на Пд;
- индивидуальное задание и календарный план выполнения Пд;
- методические указания по применению средств контроля и оценочных средств Пд;
- график консультаций.

Информационное обеспечение выполнения Пд должно включать перечень источников информации, содержащих теоретический материал по тематике Пд, изложение методик разработки устройств и проектирования подсистем ИБ иЗИ.

Должен быть предоставлен также перечень электронных образовательных ресурсов, распределенных по этапам выполнения Пд. Материально-техническое обеспечение должно содержать современные аппаратно-программные научные комплексы, современную приборную и инструментальную базу, в том числе предоставляемую научно-производственными организациями в рамках кооперации и интеграции научно-образовательной деятельности по профилю подготовки бакалавров, проектный и конструкторский инструментарий, моделирующие средства, симуляторы, имитаторы и пр. Уровень материально-технического обеспечения Пд должен позволять

эффективное применение современных методов разработки, проектирования и конструирования в сфере профессиональной деятельности студентов. Кадровое обеспечение ПдПр должно предусматривать привлечение для руководства и сопровождения специалистов исследовательских и проектных учреждений, участвующих также в организации и проведении практик и междисциплинарных научно- технических семинаров.

3.7.5. Организация и управление Пд

Руководство производственной преддипломной практикой осуществляется руководителем практики по месту ее прохождения. Общее руководство осуществляется руководителем практики от университета. По месту прохождения практики каждому студенту назначается руководитель из числа специалистов данного предприятия или организации. Руководитель практики от университета:

- устанавливает связь с руководителями практики от организации и совместно с ними составляют рабочую программу проведения практики;

- разрабатывает тематику индивидуальных заданий;

- принимает участие в распределении студентов по рабочим местам или перемещении их по видам работ;

- несет ответственность совместно с руководителем практики от организации за соблюдение студентами правил техники безопасности;

- осуществляет контроль за соблюдением сроков практики и ее содержанием;

- оказывает методическую помощь студентам при выполнении ими индивидуальных заданий и сборе материалов к ВКР;

- оценивает результаты выполнения студентами программы практики;

- проводит необходимые установочные и промежуточные консультации по выполнению программы практики.

Руководитель по месту практики:

- контролирует организацию практики в соответствии с программой практики;

- создает необходимые условия для выполнения студентами программы практики;

- оказывает помощь студентам в подборе необходимых материалов для выполнения индивидуальных заданий;

- предоставляет отзыв о работе и качестве подготовленного студентом отчета по окончании практики.

Перед началом преддипломной практики руководителем практики от университета проводится организационное собрание группы студентов. На нем студентов знакомят с целями и задачами практики, местами и сроками проведения практики, отчетностью,

возможностями по консультации и т.д. на основании приказа о проведении преддипломной практики, с указанием студентов и руководителей, мест и условий прохождения практики. Приказ утверждается ректором университета. Инструктаж по технике безопасности должен быть проведен на предприятии (организации), в которую студент направлен на практику. Руководитель практики разрабатывает и утверждает у руководителя практики от университета задание на Пд и календарный план выполнения. По итогу преддипломной практики студенты подготавливают отчет, в котором отражается содержание выполненной работы и уровень освоения компонентов закрепленных компетенций.

Приложение 1

АННОТАЦИЯ ПРОГРАММЫ ПРАКТИКИ

Производственная преддипломная

Практика реализуется *кафедрой информационной безопасности* на базе организации, в соответствии с договором о практике.

Производственная преддипломная практика (Пд) является одним из разделов составляющей образовательной программы (ОП) и формирует у студентов компетенции в сфере профессиональной деятельности.

Цель производственной преддипломной практики: Преддипломная практика направлена на расширение и углубление теоретических знаний, формирование умений и навыков выполнения разработки и проектирования в профессиональной сфере, подготовки технических отчетных документов, окончательную формулировку темы и содержания выпускной квалификационной работы (ВКР). Состоит в формировании заданных общекультурных, профессиональных и профессионально-специализированных компетенций, компетенций, обеспечивающих подготовку студентов к практической реализации эксплуатационных и экспериментально-исследовательских работ в области обеспечения информационной безопасности и защиты информации (ИБ и ЗИ).

Задачи преддипломной практики:

- выполнение этапов работы, определенных индивидуальным заданием, календарным планом, формой представления отчетных материалов и обеспечивающих выполнение планируемых в компетентностном формате результатов;

- окончательное формулирование темы, содержания и перечня материалов, в том числе графических, выпускной квалификационной работы;

- оформление отчета, содержащего материалы этапов и раскрывающего уровень освоения заданного перечня компетенций;

- подготовка и проведение защиты полученных результатов.

Практика направлена на формирование универсальных, общепрофессиональных, общепрофессиональных компетенций, соответствующие выбранной направленности программы бакалавриата по профилю "Организация и технологии защиты информации" и профессиональных компетенций, обеспечивающих подготовку студентов к практической реализации эксплуатационных, организационно-управленческих, проектно-технологических и экспериментально-исследовательских работ в области обеспечения информационных и коммуникационных технологий (в сфере техники и технологии, охватывающих совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере):

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)
ОПК-12. Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	ОПК-12.1. Знает принципы формирования политики информационной безопасности в информационных системах; основные этапы процесса проектирования и общие требования к содержанию проекта ОПК-12.2. Умеет определять информационную инфраструктуру и информационные ресурсы организации, подлежащих защите; анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации ОПК-1.3. Владеет навыками по разработке основных показателей технико-экономического обоснования соответствующих проектных решений
ОПК-2.1. Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба	ОПК-2.1.1. Умеет анализировать угрозы безопасности информации, оценивать информационные риски; применять аналитические и компьютерные модели автоматизированных систем и систем защиты информации; анализировать программные и программно-аппаратные решения при проектировании системы защиты информации с целью выявления уязвимостей ОПК-2.1.2. Умеет разрабатывать предложения по совершенствованию системы управления защиты информации, осуществлять планирование и организацию работы персонала с учетом требований по защите информации ОПК-2.1.3. Владеет навыками выработки рекомендаций для решения о модернизации системы защиты информации
ОПК-2.2 Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы	ОПК-2.2.1 Знает организационные меры по защите информации, основные методы управления защитой информации ОПК-2.2.2 Умеет разрабатывать предложения по совершенствованию системы управления защиты информации, осуществлять планирование и организацию работы персонала с учетом требований по защите информации ОПК-2.2.3 Владеет навыками выработки рекомендаций для решения о модернизации системы защиты информации
ОПК-2.3. Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности	ОПК-2.3.1 Знает национальные, межгосударственные и международные стандарты в области защиты информации, нормативные правовые акты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти в области внедрения и эксплуатации средств защиты информации ОПК-2.3.2 Умеет документировать процедуры и результаты контроля функционирования системы защиты информации; проводить испытания программно-

	технических средств защиты информации от НСД и специальных воздействий на соответствие требованиям по безопасности информации и техническим условиям ОПК-2.3.3 Владеет навыками внесения изменений в эксплуатационную документацию и организационно-распорядительные документы по системе защиты информации; навыками разработки программ и методик испытаний опытного образца программно-технического средства защиты информации от НСД и специальных воздействий на соответствие техническим условиям
ОПК-2.4 Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами	ОПК-2.4.1 Знает критерии оценки защищенности объекта информатизации, технические средства контроля эффективности мер защиты информации, методы измерений, контроля и технических расчетом характеристик программно-аппаратных средств защиты информации ОПК-2.4.2 Умеет осуществлять контроль обеспечения уровня защищенности объектов информатизации ОПК-2.4.3 Владеет навыками оценки защищенности объектов информатизации с помощью типовых программных средств
ПК-7 Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	ПК-7.1 Знает разработку концепции средств и систем информатизации в защищенном исполнении, разработку технического задания на средство и/или систему информатизации в защищенном исполнении ПК-7.2 Умеет разрабатывать конструкторскую и технологическую документацию на средство и/или систему информатизации в защищенном исполнении ПК-7.3 Владеет навыками разработки рабочей и эксплуатационной документации на средства и системы информатизации в защищенном исполнении
ПК-8 Способен оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	ПК-8.1 Знает нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа, проектирования средств защиты информации, сертификации средств защиты информации на соответствие требованиям по безопасности информации и аттестации объектов информатизации на соответствие требованиям по защите информации, стандарты ЕСКД, ЕСТД и ЕСПД ПК-8.2 Умеет оформлять рабочую и эксплуатационную документацию на средства и системы информатизации в защищенном исполнении ПК-8.3 Владеет навыками разработки технического проекта средства и/или системы информатизации в защищенном исполнении
ПК-9 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения	ПК-9.1 Знает нормативные правовые акты в области защиты информации, национальные, межгосударственные и международные стандарты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ПК-9.2 Владеет организационными мерами по защите

информационной безопасности по профилю своей профессиональной деятельности	информации ПК-9.3 Умеет работать с программным обеспечением с соблюдением действующих требований по защите информации
ПК-10 Способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	ПК-10.1 Знает нормативные правовые акты в области защиты информации, национальные, межгосударственные и международные стандарты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ПК-10.2 Умеет анализировать данные о назначении, функциях, условиях функционирования объектов и систем обработки информации ограниченного доступа, установленных на объектах информатизации, и характере обрабатываемой на них информации ПК-10.3 Владеет навыком разработки аналитического обоснования необходимости создания системы защиты информации в организации
ПК-11 Способен проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	ПК-11.1 Знает методики проведения теоретических исследований уровней защищенности информационной безопасности объектов и систем ПК-11.2 Умеет составлять и оформлять аналитический отчет по проведенным испытаниям, делать выводы по оценке защищенности на основании аналитического отчета ПК-11.3 Владеет навыками использования профиля защиты и задания по безопасности, формулирования выводов по оценке защищенности
ПК-12 Способен принимать участие в проведении экспериментальных исследований системы защиты информации	ПК-12.1 Знает методы и технологии проектирования, моделирования, исследования систем защиты информации ПК-12.2 Умеет выполнять сбор, обработку, анализ и систематизацию информации в области защиты информации ПК-12.3 Владеет навыками по разработке и исследованию конкретных явлений и процессов для решения расчетных и исследовательских задач
ПК-13 Способен принимать участие в формировании, организации и поддержания выполнения комплекса мер по обеспечению информационной безопасности, управлении процессом их реализации	ПК-13.1 Знает процедуру организации установки и настройки технических, программных (программно-технических) средств защиты информации, входящих в состав системы защиты информации организации, в соответствии с техническим проектом и инструкциями по эксплуатации ПК-13.2 Умеет разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы защиты информации ПК-13.3 Владеет навыками организации и сопровождения аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации
ПК-14 Способен организовывать работу	ПК-14.1 Знает организацию проведения инструктажа руководящего состава и обучения персонала по вопросам

малого коллектива исполнителей в профессиональной деятельности	защиты информации ПК-14.2 Умеет организовать работу персонала по использованию технических, программных (программно-технических) средств защиты информации ПК-14.3 Владеет навыками по осуществлению планирования и организации работы персонала с учетом требований по защите информации
ПК-15 Способен организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ПК-15.1 Знает технологический процесс защиты информации и процедуру разработки технических заданий, планов и графиков проведения работ по защите информации в соответствии с действующим нормативными и методическими документами ПК-15.2 Умеет применять национальные, межгосударственные и международные стандарты в области защиты информации, применять действующую законодательную базу в области обеспечения защиты информации, читать и понимать нормативные и методические документы по информационной безопасности на английском языке ПК-15.3 Владеет навыками по контролю над соблюдением установленного порядка выполнения работ, а также действующего законодательства Российской Федерации при решении вопросов, касающихся защиты информации

По практике предусмотрена промежуточная аттестация в форме *зачёта с оценкой*.

Общая трудоемкость практики составляет 9 зачетных единиц.

Приложение 2

ГРАФИК ПРОХОЖДЕНИЯ ПРАКТИКИ

УТВЕРЖДАЮ

Зав.кафедрой_____
«____»_____ 20__ г.

Дата (даты)	**Раздел практики**	**Отметка о выполнении**

Индивидуальное задание на практику
(составляется руководителем практики от кафедры)

_____
_____
_____
_____
_____
_____

Руководитель практики
от кафедры _____/_____
(подпись) (Ф.И.О.)

Руководитель практики
от организации _____/_____
(подпись) (Ф.И.О.)

Приложение 3

ФОРМА ТИТУЛЬНОГО ЛИСТА ОТЧЁТА

МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования

«Российский государственный гуманитарный университет»

(РГГУ)

Институт .....
Факультет .....
Кафедра .....

Отчёт о прохождении практики
вид (тип) практики

Код и наименование направления подготовки (специальности)

Наименование направленности (профиля, специализации)

Уровень квалификации выпускника *(бакалавр)*

Форма обучения *(очная, очно-заочная, заочная)*

Студента/ки __ курса
….. формы обучения
_____*(ФИО)*
Руководитель практики
_____(*ФИО)*

Москва 20 г.

Приложение 4

ОБРАЗЕЦ ОФОРМЛЕНИЯ ХАРАКТЕРИСТИКИ С МЕСТА ПРОХОЖДЕНИЯ ПРАКТИКИ

Характеристика[1]

на студента/тку __ курса _____ факультета
Российского государственного гуманитарного университета
_____ (*ФИО)*

_____ *(ФИО)* проходил/а производственную практику в _____ _____ на должности _____.

За время прохождения практики обучающийся/обучающаяся ознакомился/лась с: _____, выполнял/а _____, участвовал/а в _____ .

За время прохождения практики _____ *(ФИО)* зарекомендовал/а себя как _____ .

Оценка за прохождение практики – «_____» .

Руководитель практики
от организации _____ (*ФИО)*

(дата)

(подпись)

[1] Оформляется либо на бланке организации, либо заверяется печатью.