

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 комплексной защиты информации

ПРЕДДИПЛОМНАЯ ПРАКТИКА

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

10.03.01 Информационная безопасность

Код и наименование направления подготовки/специальности

«Организация и технологии защиты информации»

(по отрасли или в сфере профессиональной деятельности)»

Наименование направленности (профиля)/ специализации

Уровень высшего образования: *бакалавриат*

Форма обучения: *очная*

Рабочая программа практики адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2023

ПРОИЗВОДСТВЕННАЯ ПРАКТИКА (ПРЕДДИПЛОМНАЯ ПРАКТИКА)
Рабочая программа практики

Составитель:

к.и.н., доцент, заведующая кафедрой
информационной безопасности Г.А. Шевцова

УТВЕРЖДЕНО

Протокол заседания кафедры информационной безопасности
№ 9 от 17.03.2023

ОГЛАВЛЕНИЕ

1. Пояснительная записка	4
1.1. Цель и задачи практики	4
1.2. Вид и тип практики	4
1.3. Способы и места проведения практики.....	4
1.4. Вид (виды) профессиональной деятельности	4
1.5. Планируемые результаты обучения при прохождении практики, соотнесённые с индикаторами достижения компетенций:	4
1.6. Место практики в структуре образовательной программы.....	13
1.7.Объем практики	13
2. Содержание практики	13
3.Оценка результатов практики	14
3.1. Формы отчётности.....	14
3.2.Критерии выставления оценки по практике	14
3.3. Оценочные средства (материалы) для промежуточной аттестации обучающихся по практике.....	15
4. Учебно-методическое и информационное обеспечение практики.....	16
4.1. Список источников и литературы	16
4.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»	16
5. Материально-техническая база, необходимая для проведения практики	19
6. Организация практики для лиц с ограниченными возможностями здоровья	19
Приложение 1. Аннотация рабочей программы практики	21
Приложение 2. График прохождения практики	23
Приложение 3. Форма титульного листа отчета о прохождении практике.....	27
Приложение 4. Образец оформления характеристики с места прохождения практики	28

1. Пояснительная записка

1.1. Цель и задачи практики

Цель практики – подготовка студента к решению практических задач обеспечения комплексной защиты информации, а также сбор, обработка и систематизация материалов, необходимых для написания выпускной квалификационной работы, т.е. приобретение как персонального практического опыта в исследуемой сфере деятельности, так и приобретение навыков самостоятельной работы по избранному виду профессиональной деятельности.

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 практики:

- закрепить основные положения теории информационной безопасности и практики защиты информации, основные положения нормативных документов в области защиты объектов информатизации;
- уметь организовывать процесс применения существующие средства защиты информации от несанкционированного доступа;
- овладеть методами синтеза и анализа систем защиты информации, закономерностями построения сложных систем защиты, навыками эксплуатации средств защиты информации, получивших широкое применение в качестве инструментария в современных системах информационной безопасности на предприятии;
- сбор, обработка и систематизация материалов, необходимых для написания выпускной квалификационной работы

1.2. Вид и тип практики

Вид практики – производственная практика, тип практики – преддипломная практика.

1.3. Способы и места проведения практики

Способы проведения практики: стационарная, выездная.

Стационарная практика проводится в структурных подразделениях РГГУ, предназначенных для практической подготовки или в профильных организациях, расположенных на территории г. Москвы, на основании договора, заключаемого между РГГУ и профильной организацией.

Выездная практика проводится в профильных организациях различных регионов Российской Федерации, на основании договора, заключаемого между РГГУ и профильной организацией.

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-2.1 Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источни-	ОПК-2.1.1. Умеет анализировать угрозы безопасности информации, оценивать информационные риски; применять аналитические и компьютерные модели автоматизированных систем и систем защиты информации; анализировать про-	<i>Знать:</i> терминологию процессов и систем защиты информации; основные методы моделирования процессов и систем защиты информации, основные принципы и приемы построения моделей; основные норма-

<p>ков информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба</p>	<p>граммные и программно-аппаратные решения при проектировании системы защиты информации с целью выявления уязвимостей</p> <p>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</p> <p>ОПК-2.1.3. Владеет навыками выработки рекомендаций для решения о модернизации системы защиты информации</p>	<p>тивно-правовые акты, регламентирующие вопросы определения и моделирования угроз безопасности информации в информационных системах; методологии и средства процессов и систем.</p> <p><i>Уметь:</i> 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.</p> <p><i>Владеть:</i> 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.</p>
<p>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</p>	<p>ОПК-2.2.1 Знает организационные меры по защите информации, основные методы управления защитой информации</p> <p>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</p> <p>ОПК-2.2.3 Владеет навыками выработки рекомендаций для решения о модернизации системы защиты информации</p>	<p><i>Знать:</i> основные технические характеристики информационных систем; основные направления политики предприятий в области обеспечения комплексной безопасности; особенности организационно-правового регулирования в области обеспечения комплексной безопасности.</p> <p><i>Уметь:</i> оценивать возможную величину ущерба от реализации угроз;</p> <p><i>Владеть:</i> методикой по разработке технических решений по обеспечению безопасности объекта защиты; классификацией защищаемой информации по видам тайны; навыками подбора,</p>

		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	<p>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</p> <p>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</p> <p>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</p>	<p><i>Знать:</i> 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</p> <p><i>Уметь:</i> оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов; оценивать используемые системы документооборота с точки зрения обеспечения защищенности обрабатываемой информации и юридической силы электронных данных.</p> <p><i>Владеть:</i> навыками использовать основы правовых знаний в различных сферах деятельности; основной терминологией, методами и основными алгоритмами реализации процесса</p>
ОПК-2.4 Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами	<p>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</p> <p>ОПК-2.4.2 Умеет осуществлять контроль обеспечения уровня защищенности объектов ин-</p>	<p><i>Знать:</i> 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</p>

	<p>форматизации ОПК-2.4.3 Владеет навыками оценки защищенности объектов информатизации с помощью типовых программных средств</p>	<p><i>Уметь:</i> 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. <i>Владеть:</i> 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.</p>
Тип задач профессиональной деятельности: проектно-технологический		
<p>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</p>	<p>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</p>	<p><i>Знать:</i> порядок проектирования подсистем и средств обеспечения информационной безопасности. <i>Уметь:</i> проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности. <i>Владеть:</i> навыками участия в проведении технико-экономического обоснования проектных решений.</p>
<p>ПК-8 Способен оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов</p>	<p>ПК-8.1 Знает нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа, проектирования средств защиты ин-</p>	<p><i>Знать:</i> основные руководящие, методические и нормативные документы по организационно-технической защите информации <i>Уметь:</i> описывать объекты</p>

	<p>формации, 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</p> <p>ПК-8.2 Умеет оформлять рабочую и эксплуатационную документацию на средства и системы информатизации в защищенном исполнении</p> <p>ПК-8.3 Владеет навыками разработки технического проекта средства и/или системы информатизации в защищенном исполнении</p>	<p>защиты; выявлять источники угроз безопасности ресурсам организации; оценивать возможную величину ущерба от реализации угроз;</p> <p><i>Владеть:</i> методикой по разработке нормативных документов, технических решений по обеспечению безопасности объекта защиты</p>
Тип задач проф. деятельности: экспериментально-исследовательский		
<p>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</p>	<p>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</p> <p>ПК-9.2 Владеет организационными мерами по защите информации</p> <p>ПК-9.3 Умеет работать с программным обеспечением с соблюдением действующих требований по защите информации</p>	<p><i>Знать:</i> основную научно-техническую литературу, нормативные и методические документы в области обеспечения информационной безопасности</p> <p><i>Уметь:</i> оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов</p> <p><i>Владеть:</i> навыками использовать основы правовых знаний в различных сферах деятельности</p>
<p>ПК-10 Способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности</p>	<p>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</p> <p>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</p> <p>ПК-10.3 Владеет навыком разра-</p>	<p><i>Знать:</i> основные нормативные правовые акты в области защиты информации</p> <p><i>Уметь:</i> организовать согласование и утверждение документации по выполняемым работам с учетом требований нормативных документов в области информационной безопасности</p> <p><i>Владеть:</i> навыками по разработке аналитического обоснования необходимости создания системы защиты информации в организации с учетом требований нормативных документов в области информационной безопасности</p>

	ботки аналитического обоснования необходимости создания системы защиты информации в организации	
ПК-11 Способен проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	<p>ПК-11.1 Знает методики проведения теоретических исследований уровней защищенности информационной безопасности объектов и систем</p> <p>ПК-11.2 Умеет составлять и оформлять аналитический отчет по проведенным испытаниям, делать выводы по оценке защищенности на основании аналитического отчета</p> <p>ПК-11.3 Владеет навыками использования профиля защиты и задания по безопасности, формулирования выводов по оценке защищенности</p>	<p><i>Знать:</i> 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</p> <p><i>Уметь:</i> описывать объекты защиты; выявлять источники угроз безопасности ресурсам организации; оценивать возможную величину ущерба от реализации угроз</p> <p><i>Владеть:</i> методикой по разработке технических решений по обеспечению безопасности объекта защиты</p>
ПК-12 Способен принимать участие в проведении экспериментальных исследований системы защиты информации	<p>ПК-12.1 Знает методы и технологии проектирования, моделирования, исследования систем защиты информации</p> <p>ПК-12.2 Умеет выполнять сбор, обработку, анализ и систематизацию информации в области защиты информации</p> <p>ПК-12.3 Владеет навыками по разработке и исследованию конкретных явлений и процессов для решения расчетных и исследовательских задач</p>	<p><i>Знать:</i> методику проведения экспериментальных исследований системы защиты информации.</p> <p><i>Уметь:</i> тестировать средства защиты информации автоматизированной системы от несанкционированного доступа на соответствие установленным правилам разграничения доступа.</p> <p><i>Владеть:</i> навыками тестирования средств защиты информации автоматизированной системы от несанкционированного доступа</p>
Тип задач профессиональной деятельности: организационно-управленческий		
ПК-13 Способен принимать участие в формировании, организации и поддержания выполнения комплекса мер по обеспечению информационной безопасности, управлению процессом их реализации	<p>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</p> <p>ПК-13.2 Умеет разрабатывать и реализовывать организационные меры, обеспечивающие эффек-</p>	<p><i>Знать:</i> структуру, задачи и функции системы обеспечения информационной безопасности организаций; 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 инфор-</p>

	<p>тивность системы защиты информации</p> <p>ПК-13.3 Владеет навыками организации и сопровождения аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации</p>	<p>мационной безопасности организаций, основы менеджмента рисков нарушения информационной безопасности</p> <p><i>Уметь:</i> 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.</p> <p><i>Владеть:</i> 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</p>
<p>ПК-14 Способен организовывать работу малого коллектива исполнителей в профессиональной деятельности</p>	<p>ПК-14.1 Знает организацию проведения инструктажа руководящего состава и обучения персонала по вопросам защиты информации</p> <p>ПК-14.2 Умеет организовать работу персонала по использованию технических, программных (программно-технических) средств защиты информации</p> <p>ПК-14.3 Владеет навыками по осуществлению планирования и организации работы персонала с учетом требований по защите информации</p>	<p><i>Знать:</i> 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;</p> <p>бизнес-процессы в сфере управления персоналом и роль в них линейных менеджеров и специалистов по управлению персоналом.</p> <p><i>Уметь:</i> 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; раз-</p>

		<p>рабатывать 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.</p> <p><i>Владеть:</i> 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.</p>
<p>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</p>	<p>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</p> <p>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</p> <p>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</p>	<p><i>Знать:</i> 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 нарушения информационной безопасности; требования к системе защиты информации учреждений и предприятий и методы оценки их соблюдения.</p> <p><i>Уметь:</i> проводить анализ эффективности защиты с точки зрения ее соответствия требованиям действующих нормативных документов и лучшим практикам.</p> <p><i>Владеть:</i> навыками эффективного внедрения мер по защите информации в существующие технологические процессы обработки информации в информационных системах организаций; навыками выработки рекомендаций по составу организационно-технических</p>

		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

Практика «Преддипломная практика» относится к части, формируемой участниками образовательных отношений блока 2 «Практика» учебного плана.

Для прохождения практики необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин и прохождения практик: «Технология и методы программирования», «Информационные технологии», «Организационное и правовое обеспечение информационной безопасности», «Гуманитарные аспекты информационной безопасности», «Основы управления информационной безопасностью», «Комплексная защита объектов информатизации», «Методы принятия организационно-технических решений», «Системы электронного документооборота», «Нормативные документы и стандарты по информационной безопасности», «Методология и организация информационно-аналитической деятельности».

1.7. Объем практики

Общая трудоёмкость дисциплины составляет 9 з.е., 324 академических часа, в том числе контактная работа 36 академических часов.

Продолжительность практики составляет 6 недель.

2. Содержание практики

№	Наименование раздела	Содержание и виды работ
1.	Инструктаж по технике безопасности	Изучение локальных нормативных актов, принятых на предприятии
2.	Деятельность по защите объекта информатизации	<i>Изучить:</i> структуру предприятия, учреждения, организации, их основные функции; структуру системы управления предприятием, учреждением, организацией; информационное обеспечение управления предприятием, учреждением, организацией; структуру системы управления персоналом (расстановка кадров, должностные обязанности, система мотивации и пр.); планирование производства и сбыта средств защиты информации; механизм формирования затрат, его эффективность и механизм ценообразования; деятельность предприятия, учреждения, организации и их отдельных подразделений; основные правовые положения в области обеспечения информационной безопасности на предприятии, в учреждении, организации.
3.	Подготовка и защита	<i>Освоить:</i>

	отчёта по практике	технологии и процедуры сбора статистического и другого необходимого материала для написания выпускной квалификационной работы с написанием отчёта о прохождении практики; методы организации и управления деятельностью служб информационной безопасности на предприятии, в учреждении, организации; методики проверки защищённости объектов информатизации на соответствие требованиям нормативных документов.
--	--------------------	---

3. Оценка результатов практики

3.1. Формы отчётности

Формами отчётности по практике являются: отчёт обучающегося, характеристика с места прохождения практики.

3.2. Критерии выставления оценки по практике

Баллы/ Шкала ECTS	Оценка по практике	Критерии оценки результатов практики
100-83/ A,B	отлично	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	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	удовлетворительно	Выставляется обучающемуся, если характеристика с места прохождения практики содержит положительную оценку, отчет по оформлению и содержанию частично соответствует существующим требованиям, 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	Выставляется обучающемуся, если характеристика с места прохождения практики не содержит положительной оценки. Отчет представлен не вовремя и не соответствует существующим требованиям. Обучающийся испытывает серьёзные 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 – «неудовлетворительно».

Баллы/ Шкала ECTS	Оценка по практике	Критерии оценки результатов практики
		речических 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

Примерные индивидуальные задания на практику

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

Текущим контролем успеваемости прохождения практики является контроль посещаемости и составления отчёта.

Промежуточная аттестация – зачет с оценкой, проводится в форме защиты отчёта. Оценка выполненной работы производится по системе аттестации, принятой в РГГУ, на основе ответов студента по вопросам прохождения практики, индивидуальному заданию и другим параметрам, характеристики руководителей от организации, содержания и качества оформления отчёта. Оценка по практике приравнивается к оценкам по теоретическому обучению и учитывается при подведении итогов общей успеваемости студентов.

Студент, полностью выполнивший программу практики, получивший положительные отзывы от руководителя организации, где он проходил практику представляет отчёт по ней руководителю практики от кафедры (научному руководителю выпускной квалификационной работы). Результаты работы, выполненной в процессе прохождения практики, представляются в виде отчёта.

4. Учебно-методическое и информационное обеспечение практики

4.1. Список источников и литературы

Источники основные

1. Федеральный закон Российской Федерации от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации». [Электронный ресурс]. – Режим доступа: <http://base.garant.ru/12148555/>
2. Федеральный закон Российской Федерации от 27 июля 2006 г. №152-ФЗ «О персональных данных». [Электронный ресурс]. – Режим доступа: <https://duma.consultant.ru/page.aspx?878610>
3. Федеральный закон Российской Федерации от 6 апреля 2011 г. №63-ФЗ «Об электронной подписи». [Электронный ресурс]. – Режим доступа: <https://duma.consultant.ru/page.aspx?1551927>
4. Федеральный закон от 27 декабря 2002 г. №184-ФЗ «О техническом регулировании». [Электронный ресурс]. – Режим доступа: <https://www.garant.ru/hotlaw/federal/82403/> свободный
5. Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утв. Приказом Директора ФСБ России от 09 февраля 2005 года №66. [Электронный ресурс]. – Режим доступа: <https://base.garant.ru/187947/>
6. Федеральный закон от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_113658/
7. Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/
8. Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_40241/
9. 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/
10. 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/
11. 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/
12. 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/
13. ГОСТ Р ИСО/МЭК 15408-1,2,3-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1,2,3. [Электронный ресурс]. – Режим доступа: <https://base.garant.ru/71086050/https://base.garant.ru/71052128/https://base.garant.ru/71052126/> свободный в рамках коммерческой версии Гарант, доступной с компьютеров РГГУ
14. ГОСТ Р МЭК 61508-3-2012. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению. [Электронный ресурс]. – Режим доступа: <https://base.garant.ru/71218638/> свободный в рамках коммерческой версии Гарант, доступной с компьютеров РГГУ
15. Руководящий документ ФСТЭК России. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классифи-

кация по уровню контроля недекларированных возможностей. [Электронный ресурс]. – Режим доступа: <https://fstec.ru/component/attachments/download/294>

16. Руководящий документ ФСТЭК России. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий (Часть 1, Часть 2, Часть 3). . [Электронный ресурс]. – Режим доступа: <https://fstec.ru/component/attachments/download/293>

Литература

Основная

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>

Грушо А.А. Теоретические основы компьютерной безопасности: учеб. пособие для студентов высш. учеб. заведений / А.А. Грушо, Э.А. Применко, Е.Е. Тимонина. – М.: Академия, 2009. – 267 с.

Запечников С.В. Криптографические протоколы и их применение в финансовой и коммерческой деятельности: учеб. пособие для вузов. – М.: Горячая линия – Телеком, 2007. – 320 с.

Казарин О. В. Методология защиты программного обеспечения / О. В. Казарин; МГУ им. М. В. Ломоносова, Координац. совет по приоритетному науч. направлению «Безопасность и противодействие терроризму». – М.: МЦНМО, 2009. – 464с. – (Научные проблемы безопасности и противодействия терроризму).

дополнительная

Грибунин В.Г. Комплексная система защиты информации на предприятии: учеб. пособие для студентов вузов, обучающихся по специальностям «Организация и технология защиты информации», «Комплексная защита объектов информатизации» направления подготовки «Информационная безопасность» / В.Г. Грибунин, В.В. Чудовский. – М.: Академия, 2009. – 411 с.

Липаев В.В. Программная инженерия : методологические основы : учебник для студентов вузов, обучающихся по направлению "Бизнес-информатика" (080700) / В.В. Липаев ; Гос. ун-т Высш. шк. экономики. – М. : ТЕИС, 2006. – 605 с.

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.-Петербург. 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. Минева 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 компетентного 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). — www.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

4.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Сайт компании ООО «КриптоПро». [Электронный ресурс]. – Режим доступа: <http://www.cryptopro.ru/>

2. Сайт компании ЗАО НИП «Информзащита». [Электронный ресурс]. – Режим доступа: <http://www.infosec.ru/>

3. Сайт компании ФГУП «НТЦ «Атлас». [Электронный ресурс]. – Режим доступа: <http://web.stcnet.ru/>

4. Сайт компании ЗАО ОКБ «САПР». [Электронный ресурс]. – Режим доступа: <http://okbsapr.ru/>

5. Сайт компании ЗАО «Аладдин Р.Д.». [Электронный ресурс]. – Режим доступа: <http://www.aladdin-rd.ru/>

Национальная электронная библиотека (НЭБ) www.rusneb.ru
ELibrary.ru Научная электронная библиотека www.elibrary.ru
Электронная библиотека Grebennikon.ru www.grebennikon.ru

5. Материально-техническая база, необходимая для проведения практики

Материально-техническая база обеспечивается предприятием (организацией), где проходит практику обучающийся в соответствии с профилем подготовки и темой выпускной квалификационной работы.

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 указано:

- 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 РГГУ согласовывает с организацией (предприятием) условия и виды труда с учетом рекомендаций медико-социальной экспертизы и индивидуальной программы реабилитации инвалида. При необходимости для прохож-

дения 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 и/или в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха материалы предоставляются в форме электронного документа и/или в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата материалы предоставляются в форме электронного документа и/или в печатной форме.

Защита отчета по практике для лиц с нарушениями зрения проводится в устной форме без предоставления обучающимся 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 Минтруда России от 22.06.2015 № 386н.

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

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ПРАКТИКИ ПРОИЗВОДСТВЕННАЯ ПРАКТИКА (ПРЕДДИПЛОМНАЯ ПРАКТИКА)

Практика реализуется кафедрой комплексной защиты информации на базе предприятий, учреждений и организаций г. Москвы и Московской области, а также учебно-производственных базах предприятий по профилю подготовки будущей специальности, независимо от организационно-правовых форм этих предприятий. Практика осуществляется на основе договоров между РГГУ и предприятиями, учреждениями и организациями, в соответствии с которыми указанные предприятия, учреждения и организации обязаны предоставлять места для прохождения практики студентам Университета

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, 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

Практика направлена на формирование универсальных, общепрофессиональных, а также профессиональных компетенций, соответствующих проектно-технологическому, организационно-управленческому и эксплуатационному видам профессиональной деятельности:

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-2.2 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-2.3. Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности

ОПК-2.4 Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами

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-8 Способен оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов

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-10 Способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности

ПК-11 Способен проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов

ПК-12 Способен принимать участие в проведении экспериментальных исследований системы защиты информации

ПК-13 Способен принимать участие в формировании, организации и поддержания выполнения комплекса мер по обеспечению информационной безопасности, управлению процессом их реализации

ПК-14 Способен организовывать работу малого коллектива исполнителей в профессиональной деятельности

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

По практике предусмотрена промежуточная аттестация в форме зачёта с оценкой.

Общая трудоёмкость практики составляет 9 зачётных единиц.

МИНОБРНАУКИ РОССИИ



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

УТВЕРЖДАЮ
заведующий кафедрой, УНЦ/отделения
_____/_____/_____
подпись И.О. Фамилия
« ____ » _____ 20 ____ г.

кафедра/учебно-научный центр/отделение _____
(наименование)

направление подготовки/специальность _____
(код; наименование)

направленность (профиль)/специализация _____
(наименование)

ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ НА ПРАКТИКУ

Фамилия, Имя, Отчество обучающегося _____

курс _____ форма обучения _____

вид практики _____

тип практики _____

сроки практики с « ____ » _____ 20 ____ г. по « ____ » _____ 20 ____ г.

МЕСТО практики _____
(полное название организации; структурного подразделения)

Реквизиты договора
о прохождении практической подготов-
ке
(при проведении практической подготовки в организации)

Дата заключения Договора
« ____ » _____ 20 ____ г.
регистрационный номер № _____

Содержание индивидуального задания

Задание на практику составил:
руководитель практики от РГГУ

_____ « ___ » _____ 20___ г.
(уч. степень, уч. звание, должность) (подпись) (И.О. Фамилия) (дата)

Согласовано (при проведении практики в профильной организации):
руководитель практики от профильной организации

_____ « ___ » _____ 20___ г.
(должность) (подпись) (И.О. Фамилия) (дата)

Задание на практику принял:
обучающийся

_____ « ___ » _____ 20___ г.
(подпись) (И.О. Фамилия) (дата)

МИНОБРНАУКИ РОССИИ



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

УТВЕРЖДАЮ
заведующий кафедрой / УНЦ/отделения

_____/_____/_____
И.О. Фамилия

« ____ » _____ 20 ____ г.

кафедра/учебно-научный центр/отделение

(наименование)

направление подготовки/специальность

(код; наименование)

направленность (профиль)/специализация

(наименование)

РАБОЧИЙ ГРАФИК (ПЛАН) ПРОВЕДЕНИЯ ПРАКТИКИ

Фамилия, Имя, Отчество обучающегося

курс _____ форма обучения _____

вид практики _____

тип практики _____

сроки практики с « ____ » _____ 20 ____ г. по « ____ » _____ 20 ____ г.

МЕСТО практики

(полное название организации; структурного подразделения)

Реквизиты договора
о прохождении практической подготов-
ке

(при проведении практической подготовки в организации)

Дата заключения Договора

« ____ » _____ 20 ____ г.

регистрационный номер № _____

Планируемые работы

№ п/п	Содержание работы	Срок выполнения	Отметка о выполнении
1.	Оформление документов по прохождению практики	до начала практики	
2.	Проведение медицинских осмотров (обследований) в случае выполнения обучающимся работ, при выполнении которых проводятся обязательные предварительные и периодические медицинские осмотры (обследования) в соответствии с законодательством РФ (<u>при необходимости</u>)	до начала практики	
3.	Вводный инструктаж по правилам охраны труда, технике безопасности, пожарной безопасности, оформление временных пропусков для прохода в профильную организацию	в первый день практики	
4.	Выполнение индивидуального задания практики	в период практики	
5.	Консультации руководителя (-ей) практики о ходе выполнения заданий, оформлении и содержании отчета, по производственным вопросам	в период практики	
6.	Подготовка отчета по практике		
7.	Представление отчетных документов по практике руководителю практики	за три дня до окончания практики	
8.	Промежуточная аттестация по практике	в последний день практики	

Рабочий график (план) составил:

руководитель практики от РГГУ

_____ «__» _____ 20__ г.
(уч. степень, уч. звание, должность) (подпись) (И.О. Фамилия) (дата)

Согласовано (при проведении практики в профильной организации):

руководитель практики от профильной организации

_____ «__» _____ 20__ г.
(уч. степень, уч. звание, должность) (подпись) (И.О. Фамилия) (дата)

С рабочим графиком (планом) ознакомлен:

обучающийся

_____ «__» _____ 20__ г.
(подпись) (И.О. Фамилия) (дата)

ФОРМА ТИТУЛЬНОГО ЛИСТА ОТЧЕТА О ПРОХОЖДЕНИИ ПРАКТИКЕ

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)ИНСТИТУТ (ФАКУЛЬТЕТ, ОТДЕЛЕНИЕ)
Кафедра (учебно-научный центр)Отчёт о прохождении практики
Вид практики
Тип практики

Код и наименование направления подготовки/специальности

*Наименование направленности (профиля)/ специализации*Уровень высшего образования: *бакалавриат*
(указать нужное)Форма обучения: *очная*
(указать нужное)Студента/ки __ курса
очной/очно-заочной/заочной формы обучения

(ФИО)
Руководитель практики

(ФИО)

**ОБРАЗЕЦ ОФОРМЛЕНИЯ ХАРАКТЕРИСТИКИ С МЕСТА ПРОХОЖДЕНИЯ
ПРАКТИКИ****Характеристика¹**

на студента/ку __ курса _____ факультета
Российского государственного гуманитарного университета
[Ф.И.О. студента]

[Ф.И.О. студента]проходил/а [вид, тип практики]практику в [наименование организа-
ции]на должности [название должности].

За время прохождения практики обучающийся/обучающаяся ознакомился/лась
с[перечень], выполнял/а[перечень], участвовал/а в [перечень].

За время прохождения практики [Ф.И.О. студента]зарекомендовал/а себя как [уточ-
нение].

Оценка за прохождение практики – [оценка]

Руководитель практики
от организации

подпись

Ф.И.О.

Дата

¹ Оформляется либо на бланке организации, либо заверяется печатью.