МИНОБРНАУКИ РОССИИ

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

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ СИСТЕМ И БЕЗОПАСНОСТИ
Кафедра комплексной защиты информации

ПРОИЗВОДСТВЕННАЯ ПРАКТИКА (ПРЕДДИПЛОМНАЯ ПРАКТИКА)

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 2026

Производственная практика (Преддипломная практика)
Программа практики

Составитель:
Заведующий кафедрой информационной безопасности
канд.истор.наук, доцент Г.А. Шевцова

УТВЕРЖДЕНО
Протокол заседания кафедры
Информационной безопасности
№ 5 от 10.12.2025

ОГЛАВЛЕНИЕ

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 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 предложе-	*Знать:* терминологию процессов и систем защиты 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, регламенти-

	ния 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	рующие 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 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	*Знать:* основные технические характеристики информационных систем; основные направления политики предприятий в области обеспечения комплексной безопасности; особенности организационно-правового 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 эксплуа-	*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 докумен-

	тации 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	тооборота; методы обеспечения юридической силы электронных данных; основы действующего законодательства в области электронного документооборота *Уметь:* оформлять рабочую техническую документацию с учётом действующих нормативных и методических документов; оценивать используемые системы документооборота с точки зрения обеспечения защищённости 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 защищённости объекта информатизации в соответствии с нормативными документами	ОПК-2.4.1 Знает критерии оценки защищённости объекта информатизации, технические средства контроля эффективности мер защиты информации, методы измерений, контроля и технических расчётом характеристик программно-аппаратных средств защиты информации ОПК-2.4.2 Умеет осуществлять контроль обеспечения уровня защищённости объектов информатизации ОПК-2.4.3 Владеет навыками оценки защищённости 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 уяз-

		вимостей 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	*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

	технического проекта средства и/или системы информатизации в защищённом 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-техническую литературу, нормативные и методические документы в области обеспечения информационной безопасности *Уметь:* оформлять рабочую техническую документацию с учётом 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 учётом требований нормативных документов в области информационной безопасности *Владеть:* навыками по разработки аналитического обоснования необходимости создания системы защиты информации в организации с учётом требований нормативных документов в области информационной безопасности
ПК-11 Способен проводить эксперименты по заданной методике, обработку, оценку по-	ПК-11.1 Знает методики проведения теоретических исследований уровней защищённости информационной безопасности объектов и	*Знать:* назначение и основные технические характеристики информационных систем, их взаимосвязь с техническими средствами охраны и видеонаблюде-

грешности и достоверности их результатов	систем ПК-11.2 Умеет составлять и оформлять аналитический отчёт по проведённым испытаниям, делать выводы по оценке защищённости на основании аналитического отчёта ПК-11.3 Владеет навыками использования профиля защиты и задания по безопасности, формулирования выводов по оценке защищённости	ния; 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 расчётных 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 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	*Знать:* 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 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 до-

	информации	кументов 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 учётом требований по защите информации	*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 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 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	*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 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 защищённости 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 обязательной части блока 2 «Практика» учебного плана.

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	*Изучить*: 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 отчёта по практике	*Освоить*: технологию и процедуры сбора статистического и другого необходимого материала для написания выпускной квалификационной работы с написанием отчёта о прохождении практики; методы организации и управления деятельности 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 запрактикой, сформированы на уровне – «высокий».

Баллы/ Шкала ECTS	Оценка по практике	Критерии оценки результатов практики
82-68/ C	хорошо	Выставляется обучающемуся, еслихарактеристика 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 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	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, 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 других параметров, 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. Классификация по уровню контроля недекларированных возможностей. [Электронный ресурс]. – Режим доступа: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/rukovodyashchij-dokument-ot-4-iyunya-1999-g-n-114
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/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/rukovodyashchij-dokument-2003-god-4
17. Методика оценки показателя состояния технической защиты информации в информационных системах и обеспечения безопасности значимых объектов критической информационной инфраструктуры российской федерации (утв. ФСТЭК России от 11.11.2025 г.) [Электронный ресурс]: Режим доступа: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-11-noyabrya-2025-g
18. Методика анализа защищенности информационных систем, (утв. ФСТЭК России от 25.11.2025 г. [Электронный ресурс]: Режим доступа: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-25-noyabrya-2025-g

Литература

Основная

1. Гришина, Н. В. Основы информационной безопасности предприятия : учебное пособие / Н.В. Гришина. — Москва : ИНФРА-М, 2025. — 216 с. — (Высшее образование: Бакалавриат). — www.dx.doi.org/10.12737/textbook_5cf8ce075a0298.77906820. - ISBN 978-5-16-015105-2. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2198501– Режим доступа: по подписке.
2. Вдовенко, Л. А. Информационная система предприятия : учебное пособие / Л. А. Вдовенко. — 2-е изд., пераб. и доп. — Москва : Вузовский учебник : ИНФРА-М, 2024. — 304 с. - ISBN 978-5-9558-0329-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2061196 . – Режим доступа: по подписке.
3. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 5-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2026. — 384 с. — (Высшее образование). — DOI: https://doi.org/10.29039/02005-0. - ISBN 978-5-369-02005-0. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2233509. – Режим доступа: по подписке.
4. Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов : учебное пособие / Ю.Н. Сычев. — 2-е изд., перераб. и доп. — Москва : ИНФРА-М, 2024. — 602 с. — (Высшее образование). - ISBN 978-5-16-019904-7. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2021464 – Режим доступа: по подписке.

5. 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
6. 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
7. 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
8. 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
9. 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
10. Шейдаков, Н. Е. Физические основы защиты информации : учебное пособие / Н.Е. Шейдаков, О.В. Серпенинов, Е.Н. Тищенко. — Москва : РИОР : ИНФРА-М, 2026. — 204 с. — (Высшее образование). — DOI: https://doi.org/10.12737/21158. - ISBN 978-5-369-01603-9. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2084198 – Режим доступа: по подписке.
11. Кунин, Н. Т. Криптографическая защита информации: Практикум : учебное пособие / Н. Т. Кунин. — Москва : РТУ МИРЭА, 2025. — 66 с. — ISBN 978-5-7339-2447-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/493382. — Режим доступа: для авториз. пользователей.

дополнительная

12. Петровский, М. В. Тумбинская, М. В. Защита информации на предприятии : учебное пособие / М. В. Тумбинская, М. В. Петровский. - Москва ; Вологда : Инфра-Инженерия, 2024. - 144 с. - ISBN 978-5-9729-1610-8. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2169702. – Режим доступа: по подписке.
13. 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
14. 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
15. 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
16. 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
17. Ищейнов, В. Я. Организационное и техническое обеспечение информационной без-

опасности. Защита конфиденциальной информации : учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. — Москва : ИНФРА-М, 2024. — 256 с. — (Высшее образование: Специалитет). - ISBN 978-5-16-016535-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2139841 – Режим доступа: по подписке

18. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 5-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2026. — 384 с. — (Высшее образование). — DOI: https://doi.org/10.29039/02005-0. - ISBN 978-5-369-02005-0. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2233509. – Режим доступа: по подписке.
19. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2026. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2238628 – Режим доступа: по подписке.
20. Бондаренко, И. С. Информационная безопасность : учебник / И. С. Бондаренко. - Москва : Издательский Дом НИТУ «МИСиС», 2023. - 255 с. - ISBN 978-5-907560-71-0. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2148212– Режим доступа: по подписке.

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.ruwww.grebennikon.ru

5. Материально-техническая база, необходимая для проведения практики

Материально-техническая база обеспечивается предприятием (организацией), где проходит практику обучающийся в соответствие 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 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 предоставляютсяв 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 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 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 ПРОГРАММЫ ПРАКТИКИ

(*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 отчётных 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, определённых индивидуальным заданием, календарным планом, формой представления отчётных материалов и обеспечивающих выполнение планируемых в компетентностном формате результатов;
- окончательное формулирование темы, содержания и перечня материалов, в том числе графических, выпускной квалификационной работы;
- оформление отчёта, содержащего материалы этапов и раскрывающего уровень освоения заданного перечня компетенций;
- подготовка и проведение защиты полученных результатов.

В результате освоения практики обучающийся должен:

Знать:

терминологию процессов и систем защиты информации;

основные методы моделирования процессов и систем защиты информации, основные принципы и приёмы построения моделей;

основные нормативно-правовые акты, регламентирующие вопросы определения и моделирования угроз безопасности информации в информационных системах;

методологии и средства процессов и систем;

основные технические характеристики информационных систем;

основные направления политики предприятий в области обеспечения комплексной безопасности;

особенности организационно-правового регулирования в области обеспечения комплексной безопасности;

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;

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;

порядок проектирования подсистем и средств обеспечения информационной безопасности;

основные руководящие, методические и нормативные документы по организационно-технической защите информации;

основную научно-технической литературу, нормативные и методические документы в области обеспечения информационной безопасности;

основные нормативные правовые акты в области защиты информации;

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;

методику проведения экспериментальных исследований системы защиты информации;

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 информационной безопасности организаций, основы менеджмента рисков нарушения информационной безопасности;

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 менеджеров и специалистов по управлению персоналом;

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.

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;

оценивать возможную величину ущерба от реализации угроз;

оформлять рабочую техническую документацию с учётом действующих нормативных и методических документов;

оценивать используемые системы документооборота с точки зрения обеспечения защищённости обрабатываемой информации и юридической силы электронных данных;

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;

проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности;

описывать объекты защиты; выявлять источники угроз безопасности ресурсам организации;

оценивать возможную величину ущерба от реализации угроз;

оформлять рабочую техническую документацию с учётом действующих нормативных и методических документов;

организовать согласование и утверждение документации по выполняемым работам с учётом требований нормативных документов в области информационной безопасности;

описывать объекты защиты;

выявлять источники угроз безопасности ресурсам организации;

оценивать возможную величину ущерба от реализации угроз;

тестировать средства защиты информации автоматизированной системы от несанкционированного доступа на соответствие установленным правилам разграничения доступа;

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;

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;

проводить анализ эффективности защиты с точки зрения ее соответствия требованиям действующих нормативных документов и лучшим практикам.

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.

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;

навыками использовать основы правовых знаний в различных сферах деятельности; основной терминологией, методами и основными алгоритмами реализации процесса;

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 защищённости информационных процессов;

навыками использования методологии, правовых и нормативных требований и рекомендаций в области информационной безопасности;

навыками участия в проведении технико-экономического обоснования проектных решений;

методикой по разработке нормативных документов, технических решений по обеспечению безопасности объекта защиты;

навыками использовать основы правовых знаний в различных сферах деятельности;

навыками по разработки аналитического обоснования необходимости создания системы защиты информации в организации с учётом требований нормативных документов в области информационной безопасности;

методикой по разработке технических решений по обеспечению безопасности объекта защиты;

навыками тестирования средств защиты информации автоматизированной системы от несанкционированного доступа;

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;

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;

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 защищённости их информационных;

методикой оценки соответствия действующей в организации системы обеспечения информационной безопасности требованиям отраслевых стандартов.

Приложение 2. Форма титульного листа
отчета о прохождении практике

ФОРМА ТИТУЛЬНОГО ЛИСТА ОТЧЕТА О ПРОХОЖДЕНИИ ПРАКТИКЕ

МИНОБРНАУКИ РОССИИ

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

ИНСТИТУТ
ФАКУЛЬТЕТ
Кафедра / учебно-научный центр

Отчёт о прохождении практики
Наименование практики

Код и наименование направления подготовки/специальности

Наименование направленности (профиля)/ специализации

Уровень высшего образования: *бакалавриат/специалитет/магистратура*
(указать нужное)

Форма обучения: *очная, очно-заочная, заочная*
(указать нужное)

Студента/ки __ курса
очной/очно-заочной/заочной формы обучения
_____*(ФИО)*
Руководитель практики
_____(*ФИО)*

Москва 20

Приложение 3. Образец оформления характеристики
с места прохождения практики

ОБРАЗЕЦ ОФОРМЛЕНИЯ ХАРАКТЕРИСТИКИ С МЕСТА ПРОХОЖДЕНИЯ ПРАКТИКИ

Характеристика[1]
на студента/ку __ курса _____ факультета
Российского государственного гуманитарного университета
[Ф.И.О. студента]

[Ф.И.О. студента] проходил/а [наименование практики] практику в [наименование организации] 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 [уточнение].

Оценка за прохождение практики – [оценка]

Руководитель практики
от организации _____ _____
подпись Ф.И.О.

Дата

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