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

«Безопасность автоматизированных систем
(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:
Кандидат технических наук, доцент, зав. кафедрой КЗИ Д.А. Митюшин

УТВЕРЖДЕНО
Протокол заседания кафедры
комплексной защиты информации
№ 5 от 25.12.2025 г.

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 10
1.7.Объем практики 11
2. Содержание практики 11
3.Оценка результатов практики 11
3.1. Формы отчётности 11
3.2.Критерии выставления оценки по практике 11
3.3. Оценочные средства (материалы) для промежуточной аттестации обучающихся по практике 12
4. Учебно-методическое и информационное обеспечение практики 13
4.1. Список источников и литературы 13
4.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» 13
5. Материально-техническая база, необходимая для проведения практики 15
6. Организация практики для лиц с ограниченными возможностями здоровья 15
Приложение 1. Аннотация рабочей программы практики 18
Приложение 2. График прохождения практики 21
Приложение 3. Форма титульного листа отчета о прохождении практике**Ошибка! Закладка не определена.**
Приложение 4. Образец оформления характеристики с места прохождения практики**Ошибка! Закладка не определена.**

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

Задачи практики:

- закрепить основные положения теории информационной безопасности и практики защиты информации, основные положения нормативных документов в области комплексной защиты объектов информатизации;
- уметь применять 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

Проектно-технологический, организационно-управленческий и эксплуатационный.

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

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	ОПК-12.1 Знает принципы формирования политики информационной безопасности в информационных системах; основные этапы процесса проектирования и общие требования к содержанию проекта	Знать: • принципы формирования политики информационной безопасности в информационных системах; • основные этапы процесса проектирования системы защиты информации и общие требования к содержанию проекта
	ОПК-12.2 Умеет определять информационную инфраструктуру и ин-	Уметь: • определять информационную инфраструктуру и информацион-

	формационные ресурсы организации, подлежащих защите; анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации	ные ресурсы организации, подлежащих защите; • анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации
	ОПК-12.3 Владеет навыками по разработке основных показателей технико-экономического обоснования соответствующих проектных решений	Владеть: • навыками разработки основных показателей технико-экономического обоснования проектных решений по защите информации
ОПК-4.1 Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах;	ОПК-4.1.1 Знает нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	Знать: • нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации
	ОПК-4.1.2 Умеет разрабатывать документы в области обеспечения безопасности информации в автоматизированной системе при ее эксплуатации (включая управление инцидентами информационной безопасности)	Уметь: • разрабатывать документы в области обеспечения безопасности информации в АС при ее эксплуатации (включая управление инцидентами информационной безопасности);
	ОПК-4.1.3 Владеет навыками планирования мероприятий по обеспечению защиты информации и организацию работы персонала автоматизированной системы с учётом требований по защите информации	Владеть: • навыками планирования мероприятий по обеспечению защиты информации и организации работы персонала АС с учётом требований по защите информации
ОПК-4.2 Способен администрировать операционные системы, системы управления базами данных, вычислительные сети	ОПК-4.2.1 Знает средства, методы и протоколы идентификации, аутентификации и авторизации	Знать: • средства, методы и протоколы идентификации, аутентификации и авторизации субъектов в АС.
	ОПК-4.2.2 Умеет устанавливать и настраивать операционные системы, системы управления базами данных, компьютерные сети и программные системы с учётом требований по обеспечению защиты информации	Уметь: • устанавливать и настраивать операционные системы, системы управления базами данных, компьютерные сети и программные комплексы с учётом требований по обеспечению защиты информации
	ОПК-4.2.3 Владеет навыками управления полномочиями пользователей	Владеть: • навыками управления полномочиями пользователей
ОПК-4.3 Способен выполнять работы по установке, настройке, админи-	ОПК-4.3.1 Знает требования по установке, настройке, администрированию и обслуживанию про-	Знать: • требования по настройке, администрированию и обслуживанию программно-аппаратных и тех-

стрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем	граммно-аппаратных и технических средств защиты информации автоматизированных систем	нических средств защиты информации автоматизированных систем
	ОПК-4.3.2 Умеет настраивать программное обеспечение системы защиты информации, выявлять и анализировать уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации	Уметь: • настраивать программное обеспечение системы защиты информации, выявлять и анализировать уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации
	ОПК-4.3.3 Владеет навыками по осуществлению планирования и организации работы персонала автоматизированной системы с учётом требований по защите информации	Владеть: • навыками планирования и организации работы персонала автоматизированной системы с учётом требований по защите информации
ОПК-4.4 Способен осуществлять диагностику и мониторинг систем защиты автоматизированных систем	ОПК-4.4.1 Знает критерии оценки защищённости автоматизированной системы, основные угрозы безопасности информации и модели нарушителя в автоматизированных системах	Знать: • критерии оценки защищённости автоматизированной системы, основные угрозы безопасности информации и модели нарушителя в автоматизированных системах
	ОПК-4.4.2 Умеет контролировать уровень защищённости в автоматизированных системах, регистрировать и анализировать события, связанные с защитой информации в автоматизированных системах	Уметь: • контролировать уровень защищённости информации в автоматизированных системах, • регистрировать и анализировать события, связанные с защитой информации в автоматизированных системах
	ОПК-4.4.3 Владеет навыками проведения аудита защищённости информации в автоматизированных системах	Владеть: • навыками план проведения аудита защищённости информации в автоматизированных системах
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 защищённом исполнении, разработку технического задания на средство и/или систему информатизации в защищённом исполнении	Знать: • правила и порядок разработки концепции средств и систем информатизации в защищённом исполнении, • правила и порядок разработки технического задания на средство и/или систему информатизации в защищённом исполнении,
	ПК-7.2 Умеет разрабатывать конструкторскую и техноло-	Уметь: • разрабатывать конструкторскую и технологическую документа-

	гическую документацию на средство и/или систему информатизации в защищённом исполнении	цию на средство и/или систему информатизации в защищённом исполнении на базы данных
	ПК-7.3 Владеет навыками разработки рабочей и эксплуатационной документации на средства и системы информатизации в защищённом исполнении	Владеть: • навыками разработки рабочей и эксплуатационной документации на средства и системы информатизации в защищённом исполнении
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	Знать: • 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 Умеет работать с программным обеспечением с соблюдением действующих требований по защите информации	Уметь: • работать с программным обеспечением с соблюдением действующих требований по защите информации
	ПК-9.3 Владеет организационными мерами по защите информации	Владеть: • организационными мерами по защите информации
Тип задач профессиональной деятельности**:** организационно-управленческий		
ПК-3 Способен управлять защитой информации в автоматизированных системах	ПК-3.1 Знает основные методы управления защитой информации, информационные ресурсы автоматизированных систем, подлежащие защите; основные угрозы безопасности информации, модели нарушителя в автоматизированных системах	Знать: • основные методы управления защитой информации, информационные ресурсы автоматизированных систем, подлежащие защите; • основные угрозы безопасности информации и модели нарушителя в автоматизированных системах
	ПК-3.2 Умеет разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем; классифицировать и оценивать угрозы безопасности информации; оценивать информационные риски в автоматизированных системах	Уметь: • разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем; • классифицировать и оценивать угрозы безопасности информации; • оценивать информационные риски в автоматизированных системах
	ПК-3.3	Владеть:

	Владеет навыками составления комплекса правил, процедур, практических приёмов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе	• навыками составления комплекса правил, процедур, практических приёмов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе
ПК-8 Способен осуществлять мониторинг и аудит защищённости информации в автоматизированных системах	ПК-8.1 Знает основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах, организационные меры по защите информации	Знать: • основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах, • организационные меры по защите информации
	ПК-8.2 Умеет анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах; вести протоколы и журналы учёта при осуществлении аудита систем защиты информации автоматизированных систем	Уметь: • анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах; • вести протоколы и журналы учёта при осуществлении аудита систем защиты информации автоматизированных систем
	ПК-8.3 Владеет навыками выработки рекомендаций для принятия решения о модернизации системы защиты информации автоматизированной системы	Владеть: • навыками выработки рекомендаций для принятия решения о модернизации системы защиты информации автоматизированной системы
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	Знать: • 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	Уметь: • анализировать данные о назначении, функциях, условиях функционирования объектов и систем обработки информации ограниченного доступа, установленных на объектах информатизации, и

	объектах информатизации, и характере обрабатываемой на них информации	характере обрабатываемой на них информации
	ПК-10.3 Владеет навыком разработки аналитического обоснования необходимости создания системы защиты информации в организации	Владеть: • навыками разработки аналитического обоснования необходимости создания системы защиты информации в организации
Тип задач профессиональной деятельности**:** эксплуатационный		
ПК-4 Способен обеспечивать работоспособность систем защиты информации при возникновении нештатных ситуаций	ПК-4.1 Знает методы и способы обеспечения отказоустойчивости автоматизированных систем, содержание и порядок деятельности персонала по эксплуатации защищённых автоматизированных систем и подсистем безопасности автоматизированных систем	Знать: • методы и способы обеспечения отказоустойчивости автоматизированных систем, содержание и порядок деятельности персонала по эксплуатации защищённых автоматизированных систем и подсистем безопасности автоматизированных систем
	ПК-4.2 Умеет применять типовые программные средства резервирования и восстановления информации, средства обеспечения отказоустойчивости в автоматизированных системах	Уметь: • применять типовые программные средства резервирования и восстановления информации, средства обеспечения отказоустойчивости в автоматизированных системах
	ПК-4.3 Владеет навыками обнаружения, устранения неисправностей в работе системы защиты информации автоматизированной системы, резервирования программного обеспечения, технических средств, каналов передачи данных автоматизированной системы управления на случай возникновения нештатных ситуаций	Владеть: • навыками обнаружения, устранения неисправностей в работе системы защиты информации автоматизированной системы, резервирования программного обеспечения, технических средств, каналов передачи данных автоматизированной системы управления на случай возникновения нештатных ситуаций
ПК-11 Способен проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	ПК-11.1 Знает методики проведения теоретических исследований уровней защищённости информационной безопасности объектов и систем	Знать: • методики проведения теоретических исследований уровней защищённости информационной безопасности объектов и систем
	ПК-11.2 Умеет составлять и оформлять аналитический отчёт по проведённым испытаниям, делать выводы по оценке защищённости на основании аналитического отчёта	Уметь: • составлять и оформлять аналитический отчёт по проведённым испытаниям, делать выводы по оценке защищённости на основании аналитического отчёта
	ПК-11.3 Владеет навыками использо-	Владеть: • навыками использования профи-

	вания профиля защиты и задания по безопасности, формулирования выводов по оценке защищённости	ля защиты и задания по безопасности, формулирования выводов по оценке защищённости
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	Знать: • методы и технологии проектирования, моделирования, исследования систем защиты информации
	ПК-12.2 Умеет выполнять сбор, обработку, анализ и систематизацию информации в области защиты информации	Уметь: • осуществлять 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	Владеть: • навыками разработки и исследования конкретных явлений и процессов в автоматизированных системах и системах защиты информации
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	Знать: • 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	Уметь: • разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы защиты информации
	ПК-13.3 Владеет навыками организации и сопровождения аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации	Владеть: • навыками организации и сопровождения аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации

1.6. Место практики в структуре образовательной программы

Практика «Преддипломная практика» относится к части, формируемой участниками образовательных отношений 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, анали-

Баллы/ Шкала ECTS	Оценка по практике	Критерии оценки результатов практики
		тическая 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».
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

Индивидуальные задания существенно зависят от темы ВКР студента и материально-технической базы предприятия

1. Настроить изделие «Пиранья».
2. Провести измерение зоны разведдоступности
3. Провести сканирование операционной системы с использованием сканера уязвимости MaxPatrol.

Примерные контрольные вопросы

1. Порядок включение изделия «Пиранья»

2. Что такое зона разведдоступности объекта защиты
3. Какие настройки использовались при проведении пен-теста

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. 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
7. 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
8. 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/component/attachments/download/294
9. 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

10. Методика оценки показателя состояния технической защиты информации в информационных системах и обеспечения безопасности значимых объектов критической информационной инфраструктуры российской федерации (утв. ФСТЭК России от 11.112025 г.) [Электронный ресурс]: Режим доступа: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-11-noyabrya-2025-g
11. 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. Запечников, С. В. Криптографические методы защиты информации : учебник для вузов / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — Москва : Издательство Юрайт, 2024. — 309 с. — (Высшее образование). — ISBN 978-5-534-02574-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/536453.
2. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2024. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/538066.
3. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2022. — 592 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-8199-0730-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1843022. – Режим доступа: по подписке.
4. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2024. — 400 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-369-01759-3. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2140566 (дата обращения: 23.12.2025). – Режим доступа: по подписке.
5. 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.
6. 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.
7. Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие / П.Б. Хорев. — 2-е изд., испр. и доп. — Москва : ФОРУМ : ИНФРА-М, 2026. — 352 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-557-8. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2207457 – Режим доступа: по подписке.
8. 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.
9. 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.
10. Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии : учебник для вузов / М. В. Тумбинская, М. В. Петровский. — 3-е изд., стер. —

Санкт-Петербург : Лань, 2025. — 344 с. — ISBN 978-5-507-52270-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/445253. — Режим доступа: для авториз. пользователей.

Дополнительная

1. Малюк, А. А. Теория защиты информации / А.А. Малюк. - Москва : Гор. линия-Телеком, 2012. - 184 с.: ил.; . ISBN 978-5-9912-0246-6, 500 экз. - Текст : электронный. - URL: https://znanium.com/catalog/product/367555. – Режим доступа: по подписке.

2. Ищейнов, В. Я. Организационное и техническое обеспечение информационной безопасности. 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

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. 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.

5. 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.ru www.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 психоло-

го-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

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

Задачи:

- закрепить основные положения теории информационной безопасности и практики защиты информации, основные положения нормативных документов в области комплексной защиты объектов информатизации;
- уметь применять 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.

В результате освоения практики обучающийся должен:

Знать:

• принципы формирования политики информационной безопасности в информационных системах;

• основные этапы процесса проектирования системы защиты информации и общие требования к содержанию проекта

• нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации

• средства, методы и протоколы идентификации, аутентификации и авторизации субъектов в АС.

• требования по настройке, администрированию и обслуживанию программно-аппаратных и технических средств защиты информации автоматизированных систем

• критерии оценки защищённости автоматизированной системы, основные угрозы безопасности информации и модели нарушителя в автоматизированных системах

• правила и порядок разработки концепции средств и систем информатизации в защищённом исполнении,

• правила и порядок разработки технического задания на средство и/или систему информатизации в защищённом исполнении,

• 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

• основные методы управления защитой информации, информационные ресурсы автоматизированных систем, подлежащие защите;

• основные угрозы безопасности информации и модели нарушителя в автоматизированных системах

• основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах,

• организационные меры по защите информации

• 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

• методы и способы обеспечения отказоустойчивости автоматизированных систем, содержание и порядок деятельности персонала по эксплуатации защищённых автоматизированных систем и подсистем безопасности автоматизированных систем

• методики проведения теоретических исследований уровней защищённости информационной безопасности объектов и систем

• методы и технологии проектирования, моделирования, исследования систем защиты информации

• 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

Уметь:

• определять информационную инфраструктуру и информационные ресурсы организации, подлежащих защите;

• анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации

• разрабатывать документы в области обеспечения безопасности информации в АС при ее эксплуатации (включая управление инцидентами информационной безопасности);

• устанавливать и настраивать операционные системы, системы управления базами данных, компьютерные сети и программные комплексы с учётом требований по обеспечению защиты информации

• настраивать программное обеспечение системы защиты информации, выявлять и анализировать уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации

• контролировать уровень защищённости информации в автоматизированных системах,

• регистрировать и анализировать события, связанные с защитой информации в автоматизированных системах

• разрабатывать конструкторскую и технологическую документацию на средство и/или систему информатизации в защищённом исполнении на базы данных

• работать с программным обеспечением с соблюдением действующих требований по защите информации

• разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем;

• классифицировать и оценивать угрозы безопасности информации;

• оценивать информационные риски в автоматизированных системах

• анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах;

• вести протоколы и журналы учёта при осуществлении аудита систем защиты информации автоматизированных систем

• анализировать данные о назначении, функциях, условиях функционирования объектов и систем обработки информации ограниченного доступа, установленных на объектах информатизации, и характере обрабатываемой на них информации

• применять типовые программные средства резервирования и восстановления информации, средства обеспечения отказоустойчивости в автоматизированных системах

• составлять и оформлять аналитический отчёт по проведённым испытаниям, делать выводы по оценке защищённости на основании аналитического отчёта

• осуществлять сбор, обработку, анализ и систематизацию информации в области защиты информации

• разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы защиты информации

Владеть:

• навыками разработки основных показателей технико-экономического обоснования проектных решений по защите информации

• навыками планирования мероприятий по обеспечению защиты информации и организации работы персонала АС с учётом требований по защите информации

• навыками управления полномочиями пользователей

• навыками планирования и организации работы персонала автоматизированной системы с учётом требований по защите информации

• навыками план проведения аудита защищённости информации в автоматизированных системах

• навыками разработки рабочей и эксплуатационной документации на средства и системы информатизации в защищённом исполнении

• организационными мерами по защите информации

• навыками составления комплекса правил, процедур, практических приёмов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе

• навыками выработки рекомендаций для принятия решения о модернизации системы защиты информации автоматизированной системы

• навыками разработки аналитического обоснования необходимости создания системы защиты информации в организации

• навыками обнаружения, устранения неисправностей в работе системы защиты информации автоматизированной системы, резервирования программного обеспечения, технических средств, каналов передачи данных автоматизированной системы управления на случай возникновения нештатных ситуаций

• навыками использования профиля защиты и задания по безопасности, формулирования выводов по оценке защищённости

• навыками разработки и исследования конкретных явлений и процессов в автоматизированных системах и системах защиты информации

• навыками организации и сопровождения аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации

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.