МИНОБРНАУКИ РОССИИ

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

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

ЭКСПЛУАТАЦИОННАЯ ПРАКТИКА

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

10.03.01 Информационная безопасность

Код и наименование направления подготовки/специальности

«Организация и технологии защиты информации»
(по отрасли или в сфере профессиональной деятельности)»

Наименование направленности (профиля)/ специализации

Уровень высшего образования: *бакалавриат*

Форма обучения: *очная*

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

Москва 2023

ПРОИЗВОДСТВЕННАЯ ПРАКТИКА (ЭКСПЛУАТАЦИОННАЯ ПРАКТИКА)
Рабочая программа практики

Составитель:
Кандидат технических наук, и.о. зав. кафедрой КЗИ Д.А. Митюшин

Ответственный редактор
Кандидат технических наук, и.о. зав. кафедрой КЗИ Д.А. Митюшин

УТВЕРЖДЕНО
Протокол заседания кафедры
комплексной защиты информации
№ 8 от 23.03.2023

ОГЛАВЛЕНИЕ

1. Пояснительная записка 4
1.1. Цель и задачи практики 4
1.2. Вид и тип практики 4
1.3. Способы и места проведения практики 4
1.4. Вид (виды) профессиональной деятельности 4
1.5 Планируемые результаты обучения при прохождении практики, соотнесённые с индикаторами достижения компетенций: 4
1.6. Место практики в структуре образовательной программы 13
1.7.Объем практики 13
2. Содержание практики 13
3.Оценка результатов практики 13
3.1. Формы отчётности 13
3.2.Критерии выставления оценки по практике 14
3.3. Оценочные средства (материалы) для промежуточной аттестации обучающихся по практике 14
4. Учебно-методическое и информационное обеспечение практики 15
4.1. Список источников и литературы 15
4.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» 16
5. Материально-техническая база, необходимая для проведения практики 16
6. Организация практики для лиц с ограниченными возможностями здоровья 16
Приложение 1. Аннотация рабочей программы практики 19
Приложение 2. График прохождения практики ..... **Ошибка! Закладка не определена.**
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 – углубление и закрепление теоретических знаний и практических навыков в области подготовки к аттестационным испытания автоматизированной системы и проведению таких испытаний по требованиям безопасности информации.

Задачи практики:

- изучение автоматизированной системы и технологического процесса обработки информации в ней;
- формирование разрешительной системы доступа автоматизированной системы и реализация правил разграничения доступа средствами защиты информации;
- проведение тестирования средств защиты информации автоматизированной системы от несанкционированного доступа на соответствие установленным правилам разграничения доступа;
- исследование уязвимостей и угроз информационной безопасности в автоматизированной.

1.2. Вид и тип практики

Тип практики – эксплуатационная практика, вид –производственная 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

Эксплуатационный, организационно-управленческий

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

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1 Анализирует имеющиеся ресурсы и ограничения, оценивает и выбирает оптимальные способы решения поставленных задач	Знать: • имеющиеся ресурсы и ограничения, оценивает и выбирает оптимальные способы решения поставленных задач
	УК-2.2 Способность использования знаний о важнейших нормах, институтах и отраслях действующего российского права для определения круга задач и оптимальных способов их решения.	Уметь: • использования знаний о важнейших нормах, институтах и отраслях действующего российского права для определения круга задач и оптимальных способов их решения.
УК-8 Способен создавать и поддерживать в повсе-	УК-8.1 Понимает цели и задачи безопасности жизнедеятельно-	Знать: • цели и задачи безопасности жизнедеятельности, основ-

дневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	сти, основные понятия, классификацию опасных и вредных факторов среды обитания человека, правовые и организационные основы безопасности жизнедеятельности, обеспечение экологической безопасности.	ные понятия, классификацию опасных и вредных факторов среды обитания человека, правовые и организационные основы безопасности жизнедеятельности, обеспечение экологической безопасности.
	УК-8.2 Использует знания системы гражданской обороны, структуры РСЧС и их основные задачи, как часть системы общегосударственных мероприятий.	Уметь: • Использовать знания системы гражданской обороны, структуры РСЧС и их основные задачи, как часть системы общегосударственных мероприятий.
	УК-8.3 Оказывает первую помощь в очаге поражения, используя средства индивидуальной и коллективной защиты.	Владеть: • Оказанием первой помощи в очаге поражения, используя средства индивидуальной и коллективной защиты
УК-9 Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	УК-9.1 Знать основные законы и закономерности функционирования экономики; основы экономической теории, необходимые для решения профессиональных и социальных задач	Знать: • основные законы и закономерности функционирования экономики; • основы экономической теории, необходимые для решения профессиональных и социальных задач.
	УК-9.2 Уметь применять экономические знания при выполнении практических задач; принимать обоснованные экономические решения в различных областях жизнедеятельности	Уметь: • применять экономические знания при выполнении практических задач; • принимать обоснованные экономические решения в различных областях жизнедеятельности
	УК-9.3 Владеть методами выбора инструментальных средств для обработки экономических данных при решении социальных и профессиональных задач	Владеть: • методами выбора инструментальных средств для обработки экономических данных при решении социальных и профессиональных задач
УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействует им в профессиональной деятельности	УК-10.1 Определяет сущность экстремизма, терроризма, коррупционного поведения и их взаимосвязь с социальными, экономическими, политическими и иными условиями	Знать: использования знаний о важнейших нормах, институтах и действующего российского права
	УК-10.2 Анализирует правовые нормы о противодействии экстремизму, терроризму и коррупционному поведению	Уметь: Производить выборку инструментальных средств и анализ для обработки данных
	УК-11.3 Правильно применяет правовые нормы о противодействии экстремизму, тер-	Владеть: Навыками применения правовых норм в профессиональной

	роризму и коррупционному поведению	сфере
ОПК-2 Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности;	ОПК-2.1 Знает классификацию современных компьютерных систем, типовые структуры и принципы организации компьютерных сетей; назначение, функции и обобщённую структуру операционных систем; назначение и основные компоненты систем баз данных	Знать: • классификацию современных компьютерных систем, типовые структуры и принципы организации компьютерных сетей; • назначение, функции и обобщённую структуру операционных систем; • назначение и основные компоненты систем баз данных.
	ОПК-2.2 Умеет применять типовые программные средства сервисного назначения и пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети интернет	Уметь: • применять типовые программные средства сервисного назначения и пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети интернет
	ОПК-2.3 Владеет навыками поиска информации в глобальной информационной сети Интернет; применения технических и программных средств тестирования с целью определения исправности компьютера и оценки его производительности	Владеть: • навыками поиска информации в глобальной информационной сети Интернет; • навыками применения технических и программных средств тестирования с целью определения исправности компьютера и оценки его производительности
ОПК-3 Способен использовать необходимые математические методы для решения задач профессиональной деятельности	ОПК-3.1 Знает основы математики, основные понятия теории информации, основные методы оптимального кодирования источников информации	Знать: • основы математики, основные понятия теории информации, основные методы оптимального кодирования источников информации
	ОПК-3.2 Умеет исследовать функциональные зависимости, возникающие при решении стандартных прикладных задач	Уметь: • исследовать функциональные зависимости, возникающие при решении стандартных прикладных задач
	ОПК-3.3 Владеет навыками использования справочных материалов по математическому анализу, использования расчётных формул и таблиц при решении стандартных вероятностно-статистических задач, самостоятельного решения комбинированных задач	Владеть: • навыками использования справочных материалов по математическому анализу; • навыками использования расчётных формул и таблиц при решении стандартных вероятностно-статистических задач, самостоятельного решения комбинированных задач
ОПК-4 Способен применять не-	ОПК-4.1 Знает основополагающие	Знать: • основополагающие принци-

обходимые физические законы и модели для решения задач профессиональной деятельности	принципы механики, термодинамики, молекулярной физики, квантовой физики; положения электричества и магнетизма, колебаний и оптики	пы механики, термодинамики, молекулярной физики, квантовой физики; положения электричества и магнетизма, колебаний и оптики
	ОПК-4.2 Умеет делать выводы и формулировать их в виде отчёта о проделанной исследовательской работе	Уметь: • делать выводы и формулировать их в виде отчёта о проделанной исследовательской работе
	ОПК-4.3 Владеет методами расчёта	Владеть: • методами расчёта
ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;	ОПК-9.1 Знает основные понятия и задачи криптографии, математические модели криптографических систем; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации	Знать: • основные понятия и задачи криптографии, математические модели криптографических систем; • способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации.
	ОПК-9.2 Умеет применять математические модели для оценки стойкости СКЗИ и использовать в автоматизированных системах; пользоваться нормативными документами в области технической защиты информации	Уметь: • применять математические модели для оценки стойкости СКЗИ и использовать в автоматизированных системах; • пользоваться нормативными документами в области технической защиты информации
	ОПК-9.3 Владеет методами и средствами криптографической и технической защиты информации	Владеть: • методами и средствами криптографической и технической защиты информации
ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;	ОПК-10.1 Знает программно-аппаратные средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях	Знать: • программно-аппаратные средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях.
	ОПК-10.2 Умеет конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности	Уметь: • конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности
	ОПК-10.3 Владеет принципами формирования политики информационной безопасности объекта информатизации	Владеть: • принципами формирования политики информационной безопасности объекта информатизации
ОПК-11 Способен проводить экс-	ОПК-11.1 Знает стандартные вероят-	Знать: • стандартные вероятностно-

перименты по заданной методике и обработку их результатов	ностно-статистические методы анализа экспериментальных данных	статистические методы анализа экспериментальных данных.
	ОПК-11.2 Умеет строить стандартные процедуры принятия решений, на основе имеющихся экспериментальных данных	Уметь: • строить стандартные процедуры принятия решений, на основе имеющихся экспериментальных данных
	ОПК-11.3 Владеет навыками по проведению эксперимента по заданной методике с составлением итогового документа	Владеть: • навыками по проведению эксперимента по заданной методике с составлением итогового документа
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 и общие требования к содержанию проекта.
	ОПК-12.2 Умеет определять информационную инфраструктуру и информационные ресурсы организации, подлежащих защите; анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации	Уметь: • определять информационную инфра-структуру и информационные 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 по разработке основных показателей технико-экономического обоснования соответствующих проектных решений
ОПК-2.1 Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба	ОПК-2.1.1 Знает принципы построения систем защиты информации; критерии оценки эффективности и надёжности средств защиты программного обеспечения автоматизированных систем; основные угрозы безопасности информации и модели нарушителя	Знать: •принципы построения систем защиты информации; критерии оценки эффективности и надёжности средств защиты программного обеспечения автоматизированных систем; •основные угрозы безопасности информации и модели нарушителя
	ОПК-2.1.2 Умеет анализировать угрозы безопасности информации, оценивать информационные риски; применять аналитические и компьютерные модели автоматизированных систем и систем защиты информации; анализировать программные и	Уметь: •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	программно-аппаратные решения при проектировании системы защиты информации с целью выявления уязвимостей
	ОПК-2.1.3 Владеет навыками расчёта показателей эффективности защиты информации, обрабатываемой в автоматизированных системах; проведения анализа уязвимости программного и программно-аппаратных средств защиты информации	Владеть: •расчёта показателей эффективности защиты информации, обрабатываемой в автоматизированных системах; •проведения анализа уязвимости программного и программно-аппаратных средств защиты информации
ОПК-2.3 Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности	ОПК-2.3.1 Знает национальные, межгосударственные и международные стандарты в области защиты информации, нормативные правовые акты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти в области внедрения и эксплуатации средств защиты информации	Знать: •национальные, межгосударственные и международные стандарты в области защиты информации, нормативные право-вые акты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти в области внедрения и эксплуатации средств защиты информации
	ОПК-2.3.2 Умеет документировать процедуры и результаты контроля функционирования системы защиты информации; проводить испытания программно-технических средств защиты информации от НСД и специальных воздействий на соответствие требованиям по безопасности информации и техническим условиям	Уметь: •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	Владеть: •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
Тип задач профессиональной деятельности: эксплуатационный		

ПК-1 Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	ПК-1.1 Знает порядок установки, настройки и обслуживания программного обеспечения, систем управления базами данных, средств электронного документооборота и средств защиты информации	Знать: • порядок установки, настройки и обслуживания программного обеспечения, систем управления базами данных, средств электронного документооборота и средств защиты информации.
	ПК-1.2 Владеет навыками по установке, настройке и обслуживанию программного обеспечения, программно-аппаратных и технических средств защиты информации с соблюдением требований по защите информации	Владеть: • навыками по установке, настройке и обслуживанию программного обеспечения, программно-аппаратных и технических средств защиты информации с соблюдением требований по защите информации
	ПК-1.3 Умеет устанавливать программное обеспечение в соответствии с технической документацией, выполнять настройку параметров работы программного обеспечения, включая системы управления базами данных и средства электронного документооборота, формулировать правила безопасной эксплуатации	Уметь: • устанавливать программное обеспечение в соответствии с технической документацией, выполнять настройку параметров работы программного обеспечения, включая системы управления базами данных и средства электронного документооборота, формулировать правила безопасной эксплуатации
ПК-2 Способен применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	ПК-2.1 Знать архитектуру и принципы построения операционных систем, подсистем защиты информации, состав типовых конфигураций программно-аппаратных средств защиты информации, языки и системы программирования	Знать: • архитектуру и принципы построения операционных систем, подсистем защиты информации, состав типовых конфигураций программно-аппаратных средств защиты информации, языки и системы программирования.
	ПК-2.2 Умеет противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации	Уметь: • противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации
	ПК-2.3 Владеет контролем корректности функционирования программно-аппаратных средств защиты информации в операционных системах	Владеть: • контролем корректности функционирования программно-аппаратных средств защиты информации в операционных системах
ПК-3 Способен администрировать подсистемы информационной безопасности объекта защиты	ПК-3.1 Знает требования к встроенным средствам защиты информации программного обеспечения	Знать: •требования к встроенным средствам защиты информации программного обеспечения
	ПК-3.2	Уметь:

	Умеет анализировать угрозы безопасности информации программного обеспечения, формулировать и обосновывать правила безопасной эксплуатации программного обеспечения, производить проверку соответствия реальных характеристик программно-аппаратных средств защиты информации заявленным в их технической документации	•анализировать угрозы безопасности информации программного обеспечения, формулировать и обосновывать правила безопасной эксплуатации программного обеспечения, производить проверку соответствия реальных характеристик программно-аппаратных средств защиты информации заявленным в их технической документации
	ПК-3.3 Владеет навыками ликвидации обнаруженного вредоносного программного обеспечения и последствий его функционирования	Владеть: •навыками ликвидации обнаруженного вредоносного программного обеспечения и последствий его функционирования
ПК-5 Способен принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	ПК-5.1 Знает нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации	Знать: •нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации
	ПК-5.2 Умеет разрабатывать программы и методики аттестационных испытаний выделенных (защищаемых) помещений на соответствие требованиям по защите информации, проводить аттестационные испытания, оформлять заключение по результатам аттестации выделенных (защищаемых) помещений на соответствие требованиям по защите информации	Уметь: •разрабатывать программы и методики аттестационных испытаний выделенных (защищаемых) помещений на соответствие требованиям по защите информации, проводить аттестационные испытания, оформлять заключение по результатам аттестации выделенных (защищаемых) помещений на соответствие требованиям по защите информации
	ПК-5.3 Владеет навыками подготовки аттестата соответствия выделенных (защищаемых) помещений требованиям по защите информации	Владеть: •навыками подготовки аттестата соответствия выделенных (защищаемых) помещений требованиям по защите информации
ПК-6 Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных,	ПК-6.1 Знает оценки работоспособности применяемых средств защиты информации с использованием штатных средств и методик	Знать: • оценки работоспособности применяемых средств защиты информации с использованием штатных средств и методик
	ПК-6.2	Уметь:

программно-аппаратных и технических средств защиты информации	Умеет оценить эффективности применяемых средств защиты информации с использованием штатных средств и методик	• оценить эффективности применяемых средств защиты информации с использованием штатных средств и методик
	ПК-6.3 Владеет навыками определения уровня защищённости и доверия средств защиты информации	Владеть: • навыками определения уровня защищённости и доверия средств защиты информации
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: • 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	Владеть: • навыками по разработке и исследованию конкретных явлений и процессов для решения расчётных и исследовательских задач
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	Знать: • процедуру организации установки и настройки технических, программных (программ-но-технических) средств защиты информации, входящих в состав системы защиты информации организации, в соответствии с техническим проектом и инструкциями по эксплуатации.
	ПК-13.2 Владеет навыками организации и сопровождения аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации	Уметь: • навыками организации и сопровождения аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации
	ПК-13.3 Умеет разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы защиты информации	Владеть: • разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы защиты информации

1.6. Место практики в структуре образовательной программы

Практика «Эксплуатационная практика» относится к обязательной части блока 2 «Практика» учебного плана.

Для прохождения практики необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин и прохождения практик: «Технология и методы программирования», «Информационные технологии», «Методы и средства криптографической защиты информации», «Программно-аппаратные средства защиты информации», «Методы и средства защиты информации от утечки по техническим каналам», «Сети и системы передачи информации».

1.7.Объем практики

Общая трудоёмкость дисциплины составляет _3_ з.е., _108_ академических часов, в том числе контактная работа _12_ академических часов.

Продолжительность практики составляет _2_ недели.

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*: ознакомление с рабочими местами и определение направления работы изучение автоматизированной системы и технологического процесса обработки информации в ней формирование разрешительной системы доступа автоматизированной системы и реализация правил разграничения доступа средствами защиты информации проведение тестирования средств защиты информации автоматизированной системы от несанкционированного доступа на соответствие установленным правилам разграничения доступа исследование уязвимостей и угроз информационной безопасности в автоматизированной системе с последующей оценкой рисков составление и защита отчёта.
3.	Подготовка и защита отчёта по практике	*Освоить*: методы организации и управления деятельности служб информационной безопасности на предприятии, в учреждении, организации; методики проверки защищённости объектов информатизации на соответствие требованиям нормативных документов методики тестирования средств защиты информации автоматизированной системы от несанкционированного доступа на соответствие установленным правилам разграничения доступа методики исследования уязвимостей и угроз информационной безопасности в автоматизированной системе с последующей оценкой рисков..

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».
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 материально-технической базы предприятия

1. Изучить работу с АПКШ «Континент».
2. Изучить работу с комплексом радиомониторинга Кассандра К6.

3. Провести сканирование операционной системы с использованием сканера уязвимости MaxPatrol.

Примерные контрольные вопросы

1. Каким образом выполняется создание создания виртуальных частных сетейс использованием АПКШ «Континент»
2. Какие используются инструменты, позволяющие идентифицировать и анализировать цифровые стандарты связи.
3. Какие настройки использовались при проведении пен-теста

Устный опрос

Вопросы к защите отчёта по практике

1. Понятие предметной области.
2. Общие сведения о СЗИ от НСД.
3. Общие сведения об аттестации объекта информатизации
4. Общие сведения о программном обеспечении для тестирования СЗИ от НСД.
5. Общие сведения об угрозах и уязвимостях

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.

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. *Руководящий докумен*т. Защита от несанкционированного доступа к информации. Термины и определения. Утверждено решением председателя Гостехкомиссии России от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/386-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g3 , свободный. – Загл. с экрана.
2. *Руководящий документ*. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g , свободный. – Загл. с экрана.
3. *Руководящий документ*. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации. Утверждено решением председателя Государственной технической комис-

сии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/385-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g2 , свободный. – Загл. с экрана.

4. *Руководящий документ*. Средства вычислительной техники. Межсетевые экраны Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/383-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-25-iyulya-1997-g , свободный. – Загл. с экрана.
5. *Руководящий документ.* Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 4 июня 1999 г. N 114
6. *Федеральныйзакон* «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ (ред. от 19.07.2018). [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61798/ , свободный. – Загл. с экрана.

Литература
основная

1. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учеб.пособие / В.Ф. Шаньгин. — Москва : ИД «ФОРУМ» :ИНФРА-М, 2017. — 592 с. — (Высшее образование:Бакалавриат). - ISBN 978-5-8199-0411-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/546679. – Режим доступа: по подписке.
2. Защита информации : учеб.пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - Москва : РИОР :ИНФРА-М, 2018. - 392 с. - (Высшее образование:Бакалавриат; Магистратура). — https://doi.org/10.12737/4868. - ISBN 978-5-369-01378-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/937469– Режим доступа: по подписке.

4.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Варновский Н.П. Курс лекций по математической криптографии [Электронный ресурс]. – Режим доступа: http://cryptography.ru/wp-content/uploads/2014/11/varn_lectures_long.pdf .
2. Гарант [Электронный ресурс]: информационно-правовой портал. – Электрон. дан. – М.: НПП "ГАРАНТ-СЕРВИС”, сор. 2012. – Режим доступа: www.garant.ru.
3. КонсультантПлюс [Электронный ресурс]. – Электрон. дан. – М.: КонсультантПлюс, сор. 1997-2012. – Режим доступа: www.consultant.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 необхо-

димости). Гарантируется допуск в аудиторию, где проходит защита отчета, собаки-проводника при наличии документа, подтверждающего ее специальное обучение, выданного по форме и в порядке, утвержденных приказом Минтруда России от 22.06.2015 № 386н.

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

Для обучающихся с нарушениями опорно-двигательного аппарата защита итогов практики проводится в аудитории, оборудованной в соответствии с требованиями доступности. Помещения, где могут находиться люди на креслах-колясках, должны размещаться на уровне доступного входа или предусматривать пандусы, подъемные платформы для людей с ограниченными возможностями или лифты. В аудитории должно быть предусмотрено место для размещения обучающегося на коляске.

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

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫПРАКТИКИ

(вид, тип практики)

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 :углубление и закрепление теоретических знаний и практических навыков в области подготовки к аттестационным испытания автоматизированной системы и проведению таких испытаний по требованиям безопасности информации

Задачи:

- изучение автоматизированной системы и технологического процесса обработки информации в ней;
- формирование разрешительной системы доступа автоматизированной системы и реализация правил разграничения доступа средствами защиты информации;
- проведение тестирования средств защиты информации автоматизированной системы от несанкционированного доступа на соответствие установленным правилам разграничения доступа;
- исследование уязвимостей и угроз информационной безопасности в автоматизированной системе с последующей оценкой рисков..

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

- УК-2 – Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
- УК-8 – Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов
- УК-9 – Способен принимать обоснованные экономические решения в различных областях жизнедеятельности
- УК-10 – Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействует им в профессиональной деятельности
- ОПК-2 – Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности;
- ОПК-2.1 – Знает классификацию современных компьютерных систем, типовые структуры и принципы организации компьютерных сетей; назначение, функции и обобщённую структуру операционных систем; назначение и основные компоненты систем баз данных
- ОПК-2.2 – Умеет применять типовые программные средства сервисного назначения и пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети интернет
- ОПК-2.3 – Владеет навыками поиска информации в глобальной информационной сети Интернет; применения технических и программных средств тестирования с целью определения исправности компьютера и оценки его производительности

- ОПК-3 – Способен использовать необходимые математические методы для решения задач профессиональной деятельности
- ОПК-3.1 – Знает основы математики, основные понятия теории информации, основные методы оптимального кодирования источников информации
- ОПК-3.2 – Умеет исследовать функциональные зависимости, возникающие при решении стандартных прикладных задач
- ОПК-3.3 – Владеет навыками использования справочных материалов по математическому анализу, использования расчётных формул и таблиц при решении стандартных вероятностно-статистических задач, самостоятельного решения комбинированных задач
- ОПК-4 – Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности
- ОПК-4.1 – Знает основополагающие принципы механики, термодинамики, молекулярной физики, квантовой физики; положения электричества и магнетизма, колебаний и оптики
- ОПК-4.2 – Умеет делать выводы и формулировать их в виде отчёта о проделанной исследовательской работе
- ОПК-4.3 – Владеет методами расчёта
- ОПК-9 – Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;
- ОПК-9.1 – Знает основные понятия и задачи криптографии, математические модели криптографических систем; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации
- ОПК-9.2 – Умеет применять математические модели для оценки стойкости СКЗИ и использовать в автоматизированных системах; пользоваться нормативными документами в области технической защиты информации
- ОПК-9.3 – Владеет методами и средствами криптографической и технической защиты информации
- ОПК-10 – Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;
- ОПК-10.1 – Знает программно-аппаратные средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях
- ОПК-10.2 – Умеет конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности
- ОПК-10.3 – Владеет принципами формирования политики информационной безопасности объекта информатизации
- ОПК-11 – Способен проводить эксперименты по заданной методике и обработку их результатов
- ОПК-11.1 – Знает стандартные вероятностно-статистические методы анализа экспериментальных данных
- ОПК-11.2 – Умеет строить стандартные процедуры принятия решений, на основе имеющихся экспериментальных данных
- ОПК-11.3 – Владеет навыками по проведению эксперимента по заданной методике с составлением итогового документа
- ОПК-12 – Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;
- ОПК-12.1 – Знает принципы формирования политики информационной безопасности в информационных системах; основные этапы процесса проектирования и общие требования к содержанию проекта
- ОПК-12.2 – Умеет определять информационную инфраструктуру и информационные ресурсы организации, подлежащих защите; анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации

- ОПК-12.3 – Владеет навыками по разработке основных показателей технико-экономического обоснования соответствующих проектных решений
- ОПК-2.1 – Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба
- ОПК-2.1.1 – Знает принципы построения систем защиты информации; критерии оценки эффективности и надёжности средств защиты программного обеспечения автоматизированных систем; основные угрозы безопасности информации и модели нарушителя
- ОПК-2.1.2 – 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-2.1.3 – Владеет навыками расчёта показателей эффективности защиты информации, обрабатываемой в автоматизированных системах; проведения анализа уязвимости программного и программно-аппаратных средств защиты информации
- ОПК-2.3 – Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности
- ОПК-2.3.1 – Знает национальные, межгосударственные и международные стандарты в области защиты информации, нормативные правовые акты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти в области внедрения и эксплуатации средств защиты информации
- ОПК-2.3.2 – Умеет документировать процедуры и результаты контроля функционирования системы защиты информации; проводить испытания программно-технических средств защиты информации от НСД и специальных воздействий на соответствие требованиям по безопасности информации и техническим условиям
- ОПК-2.3.3 – Владеет навыками внесения изменений в эксплуатационную документацию и организационно-распорядительные документы по системе защиты информации; навыками разработки программ и методик испытаний опытного образца программно-технического средства защиты информации от НСД и специальных воздействий на соответствие техническим условиям
- ПК-1 – Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
- ПК-1.1 – Знает порядок установки, настройки и обслуживания программного обеспечения, систем управления базами данных, средств электронного документооборота и средств защиты информации
- ПК-1.2 – Владеет навыками по установке, настройке и обслуживанию программного обеспечения, программно-аппаратных и технических средств защиты информации с соблюдением требований по защите информации
- ПК-1.3 – Умеет устанавливать программное обеспечение в соответствии с технической документацией, выполнять настройку параметров работы программного обеспечения, включая системы управления базами данных и средства электронного документооборота, формулировать правила безопасной эксплуатации
- ПК-2 – Способен применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач
- ПК-2.1 – Знать архитектуру и принципы построения операционных систем, подсистем защиты информации, состав типовых конфигураций программно-аппаратных средств защиты информации, языки и системы программирования
- ПК-2.2 – Умеет противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации

- ПК-2.3 – Владеет контролем корректности функционирования программно-аппаратных средств защиты информации в операционных системах
- ПК-3 – Способен администрировать подсистемы информационной безопасности объекта защиты
- ПК-3.1 – Знает требования к встроенным средствам защиты информации программного обеспечения
- ПК-3.2 – Умеет анализировать угрозы безопасности информации программного обеспечения, формулировать и обосновывать правила безопасной эксплуатации программного обеспечения, производить проверку соответствия реальных характеристик программно-аппаратных средств защиты информации заявленным в их технической документации
- ПК-3.3 – Владеет навыками ликвидации обнаруженного вредоносного программного обеспечения и последствий его функционирования
- ПК-5 – Способен принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации
- ПК-5.1 – Знает нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации
- ПК-5.2 – Умеет разрабатывать программы и методики аттестационных испытаний выделенных (защищаемых) помещений на соответствие требованиям по защите информации, проводить аттестационные испытания, оформлять заключение по результатам аттестации выделенных (защищаемых) помещений на соответствие требованиям по защите информации
- ПК-5.3 – Владеет навыками подготовки аттестата соответствия выделенных (защищаемых) помещений требованиям по защите информации
- ПК-6 – Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации
- ПК-6.1 – Знает оценки работоспособности применяемых средств защиты информации с использованием штатных средств и методик
- ПК-6.2 – Умеет оценить эффективности применяемых средств защиты информации с использованием штатных средств и методик
- ПК-6.3 – Владеет навыками определения уровня защищённости и доверия средств защиты информации
- 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
- 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 – Владеет навыками организации и сопровождения аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации
- ПК-13.3 – Умеет разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы защиты информации

По практике предусмотрена промежуточная аттестация в форме зачёта с оценкой.

Общая трудоёмкость практики составляет 3 зачётных единиц.

Приложение 2. Индивидуальное задание на практику

МИНОБРНАУКИ РОССИИ

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

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

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

направление подготовки/специальность _____
(код; наименование)

направленность (профиль)/специализация _____
(наименование)

ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ НА ПРАКТИКУ

Фамилия, Имя, Отчество обучающегося _____

курс _____ **форма обучения** _____

вид практики _____

тип практики _____

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

МЕСТО практики _____
(полное название организации; структурного подразделения)

Реквизиты договора
о прохождении практической подготовке
(при проведении практической подготовки в организации)

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

Содержание индивидуального задания

Задание на практику составил:
руководитель практики от РГГУ

«___» _____ 20___ г.

_____ _____ _____
(уч. степень, уч. звание, должность) (подпись) (И.О. Фамилия) (дата)

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

«___» _____ 20___ г.

_____ _____ _____
(должность) (подпись) (И.О. Фамилия) (дата)

Задание на практику принял:
обучающийся «___» _____ 20___ г.

_____ _____
(подпись) (И.О. Фамилия) (дата)

Приложение 3. График проведения практики

МИНОБРНАУКИ РОССИИ

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

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

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

направление подготовки/специальность _____
(код; наименование)

направленность (профиль)/специализация _____
(наименование)

РАБОЧИЙ ГРАФИК (ПЛАН) ПРОВЕДЕНИЯ ПРАКТИКИ

Фамилия, Имя, Отчество обучающегося _____

курс _____ **форма обучения** _____

вид практики _____

тип практики _____

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

МЕСТО практики _____
(полное название организации; структурного подразделения)

Реквизиты договора
о прохождении практической подготовке
(при проведении практической подготовки в организации)

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

Планируемые работы

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

Рабочий график (план) составил:
руководитель практики от РГГУ

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

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

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

С рабочим графиком (планом) ознакомлен:
обучающийся _____ _____ «___» _____ 20___ г.
(подпись) (И.О. Фамилия) (дата)

Приложение 4. Форма титульного листа
отчета о прохождении практике

ФОРМА ТИТУЛЬНОГО ЛИСТА ОТЧЕТА О ПРОХОЖДЕНИИ ПРАКТИКЕ

МИНОБРНАУКИ РОССИИ

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

ИНСТИТУТ (ФАКУЛЬТЕТ, ОТДЕЛЕНИЕ)
Кафедра (учебно-научный центр

Отчёт о прохождении практики
Эксплуатационная практика
Производственная

10.03.01 «Информационная безопасность»
Код и наименование направления подготовки/специальности

Наименование направленности (профиля)/ специализации

Уровень высшего образования: *бакалавриат*
(указать нужное)

Форма обучения: *очная*
(указать нужное)

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

Москва 20

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 [вид, тип 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.