

**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 ДИСЦИПЛИНЫ**

*Направление подготовки 10.03.01 Информационная безопасность*

*Направленность (профили) подготовки:*

*Организация и технология защиты информации*

*Уровень квалификации выпускника – бакалавр*

Форма обучения – очная

РПД адаптирована для лиц  
с ограниченными возможностями  
здоровья и инвалидов

Москва 2021

*Эксплуатационная практика*

*Рабочая программа дисциплины*

*Составитель:*

*Кандидат военных наук, доцент кафедры КЗИ Д.Н. Баранников*

*Ответственный редактор*

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

УТВЕРЖДЕНО

Протокол заседания кафедры

комплексной защиты информации

№ 10 от 20.05.2021 г. \_\_\_\_\_

## **ОГЛАВЛЕНИЕ**

### **1. Пояснительная записка**

- 1.1 Цель и задачи практики
- 1.2. Вид (тип) практики
- 1.3. Способы, формы и места проведения практики
- 1.4. Вид (виды) профессиональной деятельности
- 1.5. Планируемые результаты обучения при прохождении практики, соотнесённые с планируемыми результатами освоения образовательной программы
- 1.6. Место практики в структуре образовательной программы
- 1.7. Объем практики

### **2. Содержание практики**

### **3. Оценка результатов практики**

- 3.1. Формы отчетности по практике
- 3.2. Критерии выставления оценок
- 3.3. Оценочные средства (материалы) для промежуточной аттестации по практике

### **4. Учебно-методическое и информационное обеспечение практики**

- 4.1. Список источников и литературы
- 4.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

### **5. Материально-техническая база, необходимая для проведения практики**

### **6. Организация практики для лиц с ограниченными возможностями здоровья**

## **Приложения**

- Приложение 1. Аннотация программы практики
- Приложение 2. Индивидуальное задание на практику
- Приложение 3. Рабочий график (план) проведения практики
- Приложение 4. Форма титульного листа отчёта
- Приложение 5. Образец оформления характеристики с места прохождения практики

## 1. Пояснительная записка

### 1.1. Цель и задачи практики

Цель практики – углубление и закрепление теоретических знаний и практических навыков в области подготовки к аттестационным испытаниям 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 системе с последующей оценкой рисков.

### 1.2. Вид (тип) практики

Эксплуатационная практика

### 1.3. Способы, формы и места проведения практики

Способы проведения практики: стационарная, выездная  
проводится в профильных организациях, расположенных на территории г. Москвы и области.  
Формы проведения практики: дискретная.

### 1.4. Вид (виды) профессиональной деятельности

Эксплуатационная практика ориентирована на экспериментально-исследовательский вид профессиональной деятельности виды профессиональной деятельности ОП ВО, на которые ориентирована практика.

1.5 Перечень планируемых результатов обучения при прохождении практики, соотнесённых 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: • использовать знания 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 повседневной жизни и в профессиональной деятельности безопасные условия	УК-8.1 Понимает цели и задачи безопасности жизнедеятельности, основные понятия, классификацию опасных и вредных факто-	Знать: • цели и задачи безопасности жизнедеятельности, основные понятия, классификацию опасных и вредных факторов среды обитания человека,

<p>жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов</p>	<p>ров среды обитания человека, правовые и организационные основы безопасности жизнедеятельности, обеспечение экологической безопасности.</p>	<p>правовые и организационные основы безопасности жизнедеятельности, обеспечение экологической безопасности.</p>
	<p>УК-8.2 Использует знания системы гражданской обороны, структуры РСЧС и их основные задачи, как часть системы общегосударственных мероприятий.</p>	<p>Уметь: ●Использовать знания системы гражданской обороны, структуры РСЧС и их основные задачи, как часть системы общегосударственных мероприятий.</p>
	<p>УК-8.3 Оказывает первую помощь в очаге поражения, используя средства индивидуальной и коллективной защиты.</p>	<p>Владеть: ●Навыками оказания первой помощи в очаге поражения, используя средства индивидуальной и коллективной защиты</p>
<p>УК-9 Способен принимать обоснованные экономические решения в различных областях жизнедеятельности</p>	<p>УК-9.1 Знать основные законы и закономерности функционирования экономики; основы экономической теории, необходимые для решения профессиональных и социальных задач</p>	<p>Знать: ●основные законы и закономерности функционирования экономики; ●основы экономической теории, необходимые для решения профессиональных и социальных задач</p>
	<p>УК-9.2 Уметь применять экономические знания при выполнении практических задач; принимать обоснованные экономические решения в различных областях жизнедеятельности</p>	<p>Уметь: ●применять экономические знания при выполнении практических задач; ●принимать обоснованные экономические решения в различных областях жизнедеятельности</p>
	<p>УК-9.3 Владеть методами выбора инструментальных средств для обработки экономических данных при решении социальных и профессиональных задач</p>	<p>Владеть: ●методами выбора инструментальных средств для обработки экономических данных при решении социальных и профессиональных задач</p>
<p>ОПК-2 Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности;</p>	<p>ОПК-2.1 Знает классификацию современных компьютерных систем, типовые структуры и принципы организации компьютерных сетей; назначение, функции и обобщенную структуру операционных систем; назначение и основные компоненты систем баз данных</p>	<p>Знать: ●классификацию современных компьютерных систем, типовые структуры и принципы организации компьютерных сетей ●назначение, функции и обобщенную структуру операционных систем ●назначение и основные компоненты систем баз данных</p>
	<p>ОПК-2.2 Умеет применять типо-</p>	<p>Уметь:</p>

	<p>вые программные средства сервисного назначения и пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети интернет</p>	<ul style="list-style-type: none"> <li>•применять типовые программные средства сервисного назначения и пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети интернет</li> </ul>
	<p><b>ОПК-2.3</b> Владеет навыками поиска информации в глобальной информационной сети Интернет; применения технических и программных средств тестирования с целью определения исправности компьютера и оценки его производительности</p>	<p>Владеть:</p> <ul style="list-style-type: none"> <li>•навыками поиска информации в глобальной информационной сети Интернет</li> <li>•применения технических и программных средств тестирования с целью определения исправности компьютера и оценки его производительности</li> </ul>
<p><b>ОПК-3</b> Способен использовать необходимые математические методы для решения задач профессиональной деятельности</p>	<p><b>ОПК-3.1</b> Знает основы математики, основные понятия теории информации, основные методы оптимального кодирования источников информации</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>•основы математики, основные понятия теории информации, основные методы оптимального кодирования источников информации</li> </ul>
	<p><b>ОПК-3.2</b> Умеет исследовать функциональные зависимости, возникающие при решении стандартных прикладных задач</p>	<p>Уметь:</p> <ul style="list-style-type: none"> <li>•исследовать функциональные зависимости, возникающие при решении стандартных прикладных задач</li> </ul>
	<p><b>ОПК-3.3</b> Владеет навыками использования справочных материалов по математическому анализу, использования расчётных формул и таблиц при решении стандартных вероятностно-статистических задач, самостоятельного решения комбинированных задач</p>	<p>Владеть:</p> <ul style="list-style-type: none"> <li>•навыками использования справочных материалов по математическому анализу, использования расчётных формул и таблиц при решении стандартных вероятностно-статистических задач, самостоятельного решения комбинированных задач</li> </ul>
<p><b>ОПК-4</b> Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности</p>	<p><b>ОПК-4.1</b> Знает основополагающие принципы механики, термодинамики, молекулярной физики, квантовой физики; положения электричества и магнетизма, колебаний и оптики</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>•основополагающие принципы механики, термодинамики, молекулярной физики, квантовой физики; положения электричества и магнетизма, колебаний и оптики</li> </ul>
	<p><b>ОПК-4.2</b> Умеет делать выводы и формулировать их в виде отчета о проделанной исследовательской работе</p>	<p>Уметь:</p> <ul style="list-style-type: none"> <li>•делать выводы и формулировать их в виде отчета о проделанной исследовательской работе</li> </ul>

	<i>ОПК-4.3</i> Владеет методами расчета	Владеть: •методами расчета
<i>ОПК-9</i> Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;	<i>ОПК-9.1</i> 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
	<i>ОПК-9.2</i> 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
	<i>ОПК-9.3</i> Владеет методами и средствами криптографической и технической защиты информации	Владеть: •методами и средствами криптографической и технической защиты информации
<i>ОПК-10</i> 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;	<i>ОПК-10.1</i> 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
	<i>ОПК-10.2</i> 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
	<i>ОПК-10.3</i> Владеет принципами формирования политики информационной безопасности объекта информатизации	Владеть: •принципами формирования политики информационной безопасности объекта информатизации
<i>ОПК-11</i> Способен проводить эксперименты по заданной методике и обработку их результатов	<i>ОПК-11.1</i> Знает стандартные вероятностно-статистические методы анализа экспериментальных данных	Знать: •стандартные вероятностно-статистические методы анализа экспериментальных данных

	<p><i>ОПК-11.2</i> Умеет строить стандартные процедуры принятия решений, на основе имеющихся экспериментальных данных</p>	<p>Уметь:</p> <ul style="list-style-type: none"> <li>•строить стандартные процедуры принятия решений, на основе имеющихся экспериментальных данных</li> </ul>
	<p><i>ОПК-11.3</i> Владеет навыками по проведению эксперимента по заданной методике с составлением итогового документа</p>	<p>Владеть:</p> <ul style="list-style-type: none"> <li>•навыками по проведению эксперимента по заданной методике с составлением итогового документа</li> </ul>
<p><i>ОПК-12</i> Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;</p>	<p><i>ОПК-12.1</i> Знает принципы формирования политики информационной безопасности в информационных системах; основные этапы процесса проектирования и общие требования к содержанию проекта</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>•принципы формирования политики информационной безопасности в информационных системах; основные этапы процесса проектирования и общие требования к содержанию проекта</li> </ul>
	<p><i>ОПК-12.2</i> Умеет определять информационную инфраструктуру и информационные ресурсы организации, подлежащих защите; анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации</p>	<p>Уметь:</p> <ul style="list-style-type: none"> <li>•определять информационную инфраструктуру и информационные ресурсы организации, подлежащих защите; анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации</li> </ul>
	<p><i>ОПК-12.3</i> Владеет навыками по разработке основных показателей технико-экономического обоснования соответствующих проектных решений</p>	<p>Владеть:</p> <ul style="list-style-type: none"> <li>•навыками по разработке основных показателей технико-экономического обоснования соответствующих проектных решений</li> </ul>
<p><i>ОПК-2.1</i> 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</p>	<p><i>ОПК-2.1.1</i> Знает принципы построения систем защиты информации; критерии оценки эффективности и надёжности средств защиты программного обеспечения автоматизированных систем; основные угрозы безопасности информации и модели нарушителя</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>•принципы построения систем защиты информации; критерии оценки эффективности и надёжности средств защиты программного обеспечения автоматизированных систем;</li> <li>•основные угрозы безопасности информации и модели нарушителя</li> </ul>
	<p><i>ОПК-2.1.2</i> Умеет анализировать угрозы безопасности информации, оценивать информационные риски; при-</p>	<p>Уметь:</p> <ul style="list-style-type: none"> <li>•анализировать угрозы безопасности информации, оценивать информационные риски; применять аналитические</li> </ul>

	<p>менять 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</p>	<p>и компьютерные модели автоматизированных систем и систем защиты информации;</p> <ul style="list-style-type: none"> <li>● анализировать программные и программно-аппаратные решения при проектировании системы защиты информации с целью выявления уязвимостей</li> </ul>
	<p><b>ОПК-2.1.3</b> Владеет навыками расчёта показателей эффективности защиты информации, обрабатываемой в автоматизированных системах; проведения анализа уязвимости программного и программно-аппаратных средств защиты информации</p>	<p>Владеть:</p> <ul style="list-style-type: none"> <li>● расчёта показателей эффективности защиты информации, обрабатываемой в автоматизированных системах;</li> <li>● проведения анализа уязвимости программного и программно-аппаратных средств защиты информации</li> </ul>
<p><b>ОПК-2.3</b> Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности</p>	<p><b>ОПК-2.3.1</b> Знает национальные, межгосударственные и международные стандарты в области защиты информации, нормативные правовые акты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти в области внедрения и эксплуатации средств защиты информации</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>● 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</li> </ul>
	<p><b>ОПК-2.3.2</b> Умеет документировать процедуры и результаты контроля функционирования системы защиты информации; проводить испытания программно-технических средств защиты информации от НСД и специальных воздействий на соответствие требованиям по безопасности информации и техническим условиям</p>	<p>Уметь:</p> <ul style="list-style-type: none"> <li>● документировать процедуры и результаты контроля функционирования системы защиты информации;</li> <li>● проводить испытания программно-технических средств защиты информации от НСД и специальных воздействий на соответствие требованиям по безопасности информации и техническим условиям</li> </ul>
	<p><b>ОПК-2.3.3</b> Владеет навыками внесения изменений в эксплуатационную документацию и организационно-</p>	<p>Владеть:</p> <ul style="list-style-type: none"> <li>● навыками внесения изменений в эксплуатационную документацию и организационно-</li> </ul>

	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	ты 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 работу 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

	<p><i>ПК-2.2</i> Умеет противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации</p>	<p>Уметь:</p> <ul style="list-style-type: none"> <li>• противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации</li> </ul>
	<p><i>ПК-2.3</i> Владеет контролем корректности функционирования программно-аппаратных средств защиты информации в операционных системах</p>	<p>Владеть:</p> <ul style="list-style-type: none"> <li>• контролем корректности функционирования программно-аппаратных средств защиты информации в операционных системах</li> </ul>
<p><i>ПК-3</i> Способен администрировать подсистемы информационной безопасности объекта защиты</p>	<p><i>ПК-3.1</i> Знает требования к встроенным средствам защиты информации программного обеспечения</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>• требования к встроенным средствам защиты информации программного обеспечения</li> </ul>
	<p><i>ПК-3.2</i> 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</p>	<p>Уметь:</p> <ul style="list-style-type: none"> <li>• 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</li> </ul>
	<p><i>ПК-3.3</i> Владеет навыками ликвидации обнаруженного вредоносного программного обеспечения и последствий его функционирования</p>	<p>Владеть:</p> <ul style="list-style-type: none"> <li>• навыками ликвидации обнаруженного вредоносного программного обеспечения и последствий его функционирования</li> </ul>
<p><i>ПК-4</i> Способен участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты</p>	<p><i>ПК-4.1</i> Знает виды политик безопасности и их формирование, разработка профилей защиты и заданий по безопасности, решения о необходимости защиты информации, содержащейся в информационной системе</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>• виды политик безопасности и их формирование, разработку профилей защиты и заданий по безопасности, решения о необходимости защиты информации, содержащейся в информационной системе</li> </ul>
	<p><i>ПК-4.2</i> Умеет формировать политики безопасности, анализировать систему с целью определения необходимого уровня защищённости</p>	<p>Уметь:</p> <ul style="list-style-type: none"> <li>• формировать политики безопасности, анализировать систему с целью определения необходимого уровня защищённости и доверия</li> </ul>

	<i>и доверия</i>	
	<p><b>ПК-4.3</b>  <i>Владеет навыками разработки руководящих документов по защите информации в организации</i></p>	<p><b>Владеть:</b>  <ul style="list-style-type: none"> <li>•навыками разработки руководящих документов по защите информации в организации</li> </ul></p>
<p><b>ПК-5</b>  <i>Способен принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации</i></p>	<p><b>ПК-5.1</b>  <i>Знает нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации</i></p>	<p><b>Знать:</b>  <ul style="list-style-type: none"> <li>•нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации</li> </ul></p>
	<p><b>ПК-5.2</b>  <i>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</i></p>	<p><b>Уметь:</b>  <ul style="list-style-type: none"> <li>•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</li> </ul></p>
	<p><b>ПК-5.3</b>  <i>Владеет навыками подготовки аттестата соответствия выделенных (защищаемых) помещений требованиям по защите информации</i></p>	<p><b>Владеть:</b>  <ul style="list-style-type: none"> <li>•навыками подготовки аттестата соответствия выделенных (защищаемых) помещений требованиям по защите информации</li> </ul></p>
<p><b>ПК-6</b>  <i>Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации</i></p>	<p><b>ПК-6.1</b>  <i>Знает оценки работоспособности применяемых средств защиты информации с использованием штатных средств и методик</i></p>	<p><b>Знать:</b>  <ul style="list-style-type: none"> <li>•оценки работоспособности применяемых средств защиты информации с использованием штатных средств и методик</li> </ul></p>
	<p><b>ПК-6.2</b>  <i>Умеет оценить эффективности применяемых средств защиты информации с использованием штатных средств и методик</i></p>	<p><b>Уметь:</b>  <ul style="list-style-type: none"> <li>•оценить эффективности применяемых средств защиты информации с использованием штатных средств и методик</li> </ul></p>
	<p><b>ПК-6.3</b>  <i>Владеет навыками опреде-</i></p>	<p><b>Владеть:</b>  <ul style="list-style-type: none"> <li>•навыками определения уровня</li> </ul></p>

	<i>ления уровня защищенности и доверия средств защиты информации</i>	<i>защищенности и доверия средств защиты информации</i>
<i>ПК-12 Способен принимать участие в проведении экспериментальных исследований системы защиты информации</i>	<i>ПК-12.1 Знает методы и технологии проектирования, моделирования, исследования систем защиты информации</i>	<i>Знать:</i> •методы и технологии проектирования, моделирования, исследования систем защиты информации
	<i>ПК-12.2 Умеет выполнять сбор, обработку, анализ и систематизацию информации в области защиты информации</i>	<i>Уметь:</i> •выполнять сбор, обработку, анализ и систематизацию информации в области защиты информации
	<i>ПК-12.3 Владеет навыками по разработке и исследованию конкретных явлений и процессов для решения расчетных и исследовательских задач</i>	<i>Владеть:</i> •навыками по разработке и исследованию конкретных явлений и процессов для решения расчетных и исследовательских задач
<i>ПК-13 Способен принимать участие в формировании, организации и поддержания выполнения комплекса мер по обеспечению информационной безопасности, управлению процессом их реализации</i>	<i>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</i>	<i>Знать:</i> •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
	<i>ПК-13.2 Владеет навыками организации и сопровождения аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации</i>	<i>Владеть:</i> •навыками организации и сопровождения аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации
	<i>ПК-13.3 Умеет разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы защиты информации</i>	<i>Уметь:</i> •разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы защиты информации

#### 1.6. Место практики в структуре образовательной программы

Практика «Эксплуатационная практика» относится блоку Б2 («Практики») обязательной части 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».

Эксплуатационная практика является важным завершающим этапом 3 курса в процессе подготовки студентов, обучающихся по направлению подготовки 10.03.01 «Информационная безопасность», профилю «Безопасность автоматизированных систем»

### 1.7. Объем практики

Объём практики составляет 114 ч, 3 зачётные единицы. Проектно-технологическая практика (далее – практика) проводится на 3 курсе (в 6 семестре) продолжительностью 2 недели (в сроки, установленные рабочим учебным планом и расписанием, в том числе контактная работа).

## 2. Содержание практики

№	Наименование раздела	Содержание и виды работ
1.	Инструктаж по технике безопасности	Изучение локальных нормативных актов, принятых на предприятии
2.	Деятельность по защите объекта информатизации	<i>Изучить:</i> 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 проведение аттестации объектов информатизации составление и защита отчёта
3.	Подготовка и защита отчёта по практике	<i>Освоить:</i> технологии 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. Отчёт составляется в электронной форме с использованием ПКП MS Office 2007 и выше и передаётся преподавателю посредством оговорённой формы связи.

### 3.2. Критерии выставления оценки по практике

Баллы/ Шкала ECTS	Оценка по практике	Критерии оценки результатов обучения по практике
100-83/ А,В	«отлично»/ «зачтено (отлично)»/ «зачтено»	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический материал, может продемонстрировать это на защите отчета по практике. 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. Свободно ориентируется в учебной и профессиональной литературе. Оценка по практике выставляется обучающемуся по результатам защиты отчета по практике. Компетенции, закреплённые за практикой, сформиро-

<b>Баллы/ Шкала ECTS</b>	<b>Оценка по прак- тике</b>	<b>Критерии оценки результатов обучения по практи- ке</b>
		ваны на уровне – «высокий».
82-68/ С	«хорошо»/ «зачтено (хоро- шо)»/ «зачтено»	Выставляется обучающемуся, если он знает теоретиче- ский и практический материал, грамотно и по существу излагает его на защите отчета по практике, не допуская существенных неточностей. Обучающийся правильно применяет теоретические по- ложения при решении практических задач профессио- нальной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёма- ми. Достаточно хорошо ориентируется в учебной и про- фессиональной литературе. Оценка по практике выставляется обучающемуся по результатам защиты отчета по практике. Компетенции, закреплённые за практикой, сформиро- ваны на уровне – «хороший».
67-50/ D,E	«удовлетвори- тельно»/ «зачтено (удовле- творительно)»/ «зачтено»	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, до- пускает отдельные ошибки на защите отчета по прак- тике. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимы- ми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по практике. Оценка по практике выставляется обучающемуся по результатам защиты отчета по практике. Компетенции, закреплённые за практикой, сформиро- ваны на уровне – «достаточный».
49-0/ F,FX	«неудовлетвори- тельно»/ не зачтено	Выставляется обучающемуся, если он не знает на базо- вом уровне теоретический и практический материал, допускает грубые ошибки на защите отчета по практи- ке. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходи- мыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной лите- ратуры по практике. Оценка по практике выставляется обучающемуся по результатам защиты отчета по практике. Компетенции на уровне «достаточный», закреплённые за практикой, не сформированы.
<b>Баллы/ Шкала ECTS</b>	<b>Оценка по дис- циплине</b>	<b>Критерии оценки результатов обучения по дисци- плине</b>
100-83/ A,B	«отлично»/ «зачтено (отлич-	Выставляется обучающемуся, если он глубоко и проч- но усвоил теоретический и практический материал,

Баллы/ Шкала ECTS	Оценка по практике	Критерии оценки результатов обучения по практике
	но)»/ «зачтено»	<p>может продемонстрировать это на занятиях и в ходе промежуточной аттестации.</p> <p>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.</p> <p>Свободно ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».</p>
82-68/ С	«хорошо»/ «зачтено (хорошо)»/ «зачтено»	<p>Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей.</p> <p>Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами.</p> <p>Достаточно хорошо ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».</p>
67-50/ D,E	«удовлетворительно»/ «зачтено (удовлетворительно)»/ «зачтено»	<p>Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации.</p> <p>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.</p> <p>Демонстрирует достаточный уровень знания учебной литературы по дисциплине.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».</p>
49-0/ F,FX	«неудовлетворительно»/ не зачтено	<p>Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении</p>

Баллы/ Шкала ECTS	Оценка по практике	Критерии оценки результатов обучения по практике
		<p>практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами.</p> <p>Демонстрирует фрагментарные знания учебной литературы по дисциплине.</p> <p>Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.</p>

3.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

#### *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

УК-2.1; УК-2.2; УК-8.1; УК-8.2; УК-8.3; УК-9.1; УК-9.2; УК-9.3; ОПК-2.1; ОПК-2.2; ОПК-2.3; ОПК-3.1; ОПК-3.2; ОПК-3.3; ОПК-4.1; ОПК-4.2; ОПК-4.3; ОПК-9.1; ОПК-9.2; ОПК-9.3; ОПК-10.1; ОПК-10.2; ОПК-10.3; ОПК-11.1; ОПК-11.2; ОПК-11.3; ОПК-12.1; ОПК-12.2; ОПК-12.3; ОПК-2.1.1; ОПК-2.1.2; ОПК-2.1.3; ОПК-2.3.1; ОПК-2.3.2; ОПК-2.3.3; ПК-1.1; ПК-1.2; ПК-1.3; ПК-2.1; ПК-2.2; ПК-2.3; ПК-3.1; ПК-3.2; ПК-3.3; ПК-4.1; ПК-4.2; ПК-4.3; ПК-5.1; ПК-5.2; ПК-5.3; ПК-6.1; ПК-6.2; ПК-6.3; ПК-12.1; ПК-12.2; ПК-12.3; ПК-13.1; ПК-13.2; ПК-13.3.

## 4. Учебно-методическое и информационное обеспечение дисциплины

### 4.1. Список источников и литературы

#### Литература

##### Основная

1. Комплексная защита информации в корпоративных системах : учеб. пособие / В.Ф. Шаньгин. — М. : ИД «ФОРУМ» : ИНФРА-М, 2017. — 592 с. — (Высшее образование: Бакалавриат). - Режим доступа: <http://znanium.com/catalog/product/546679>
2. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс] / В. Ф. Шаньгин. - М.: ДМК Пресс, 2010. - 544 с.: ил. - ISBN 978-5-94074-518-1. - Режим доступа: <http://znanium.com/catalog/product/408107>
3. Защита информации : учеб. пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М. : РИОР : ИНФРА-М, 2018. - 392 с. - (Высшее образование: Бакалавриат; Магистратура). — <https://doi.org/10.12737/4868>. - Режим доступа: <http://znanium.com/catalog/product/937469>

##### Дополнительная

1. *Руководящий документ*. 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-predsdatelja-gostekkomissii-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-predsdatelya-gostekhkommisii-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 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/385-rukovodyashchij-dokument-reshenie-predsdatelya-gostekhkommisii-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-predsdatelya-gostekhkommisii-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 недеklarированных возможностей. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 4 июня 1999 г. N 114
6. *Федеральный закон «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/](http://www.consultant.ru/document/cons_doc_LAW_61798/) , свободный. – Загл. с экрана.

#### 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](http://cryptography.ru/wp-content/uploads/2014/11/varn_lectures_long.pdf) (дата обращения: август 2019).
2. Goldreich O. Foundations of cryptography. [Электронный ресурс]. – Режим доступа: <http://www.twirpx.com/file/493751/> .
3. Гарант [Электронный ресурс]: информационно-правовой портал. – Электрон. дан. – М.: НПП "ГАРАНТ-СЕРВИС", сор. 2012. – Режим доступа: [www.garant.ru](http://www.garant.ru).
4. КонсультантПлюс [Электронный ресурс]. – Электрон. дан. – М.: КонсультантПлюс, сор. 1997-2012. – Режим доступа: [www.consultant.ru](http://www.consultant.ru).

#### 5 Материально-техническая база, необходимая для проведения практики

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

№ договора о сотрудничестве	Наименование предприятия, учреждения, организации	Дата заключения и срок действия договора	Адрес предприятия, телефон	Материально-техническое обеспечение рабочего места обучающегося
195-05-111/ФИСБ	АО «НПО «Эшелон»	01.03.2021 – 30.06.2025	Россия, 117997, Москва, ул. Электровзводская, д. 24 стр. 1, +74952232392	

195-02-78/ФИСБ	ФГБУН Институт проблем управления им. В.А. Трапезникова (ИПУ РАН)	03.06.2019 – 03.06.2022	Россия, 117997, Москва, ул. Профсоюзная, д. 65, +74953348580	
195-05-60а/ФИСБ	ФГУП «НПП «Гамма»	27.12.2018 – до особ. раст	Россия, 117393, Москва, ул. Профсоюзная, д. 78, стр. 4 +74956631684	
ПП 0518-1	ООО «НТЦ ИТ РОСА»	03.05.2018 – 31.12.2022	124498, Россия г. Москва, г. Зеленоград, пл.Шокина, д.2, стр.3, пом.У, комн. 55 +74952270280	
195-05-54/ФИСБ	Закрытое акционерное общество «Особое Конструкторское Бюро Систем Автоматизированного Проектирования»	01.09.2018 – 31.12.2022	115114, г. Москва. 2-й Кожевнический пер., д. 12 +74959947262	
195-05-74/ФИСБ	ООО «ЗАЩИТНЫЕ ТЕХНОЛОГИИ»	29.04.2019 – 29.04.2024	г. Москва, Харьковский проезд, д. 2, стр.3, ном. 5, оф.2 +74959518552	

## 6. Организация практики для лиц с ограниченными возможностями здоровья

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

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

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

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

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

При направлении инвалида и обучающегося с ОВЗ в организацию или предприятие для прохождения предусмотренной учебным планом практики Университет согласовывает с орга-

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

Для лиц с нарушениями зрения материалы предоставляются:

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

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

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

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

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

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

## АННОТАЦИЯ ПРАКТИКИ

Практика реализуется на факультете информационных систем и безопасности кафедрой комплексной защиты информации.

Цель практики – углубление и закрепление теоретических знаний и практических навыков в области подготовки к аттестационным испытаниям 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 системе с последующей оценкой рисков.

Практика направлена на формирование следующих компетенций:

- 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
  - УК-2.2 – Способность 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 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-8.1 – Понимает цели и задачи безопасности жизнедеятельности, основные 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.
  - УК-8.3 – Оказывает первую помощь 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
  - УК-9.2 – 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
- 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-4 – Способен участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты
  - ПК-4.1 – Знает виды политик безопасности и их формирование, разработка профилей защиты и заданий по безопасности, решения о необходимости защиты информации, содержащейся в информационной системе
  - ПК-4.2 – Умеет формировать политики безопасности, анализировать систему с целью определения необходимого уровня защищённости и доверия
  - ПК-4.3 – Владеет навыками разработки руководящих документов по защите информации в организации
- 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 поддержании выполнения комплекса мер по обеспечению информационной безопасности, управлению 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 оценки отчета по практике – зачёт с оценкой.

Общая трудоёмкость освоения практики составляет 3 зачётные единицы.

**Приложение 2**

приложение № 2

к Положению о практической подготовке обучающихся ФГБОУ ВО «РГГУ»

**МИНОБРНАУКИ РОССИИ**



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

**УТВЕРЖДАЮ**

И.о. заведующего кафедрой

\_\_\_\_\_/\_\_\_\_\_/\_\_\_\_\_  
подпись И.О. Фамилия

« \_\_\_\_ » \_\_\_\_\_ 20 \_\_\_\_ г.

кафедра

**Комплексной защиты информации**  
(наименование)

направление подготовки/специальность

**10.03.01 Информационная безопасность**  
(код; наименование)

направленность (профиль)/специализация

**Организация и технология защиты информации**  
(наименование)

**ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ НА ПРАКТИКУ**

Фамилия, Имя, Отчество обучающегося \_\_\_\_\_

курс

**4**

форма обучения

**очная**

вид практики

**эксплуатационная**

тип практики

**стационарная**

сроки практики

с « \_\_\_\_ » \_\_\_\_\_ 20 \_\_\_\_ г. по « \_\_\_\_ » \_\_\_\_\_ 20 \_\_\_\_ г.

МЕСТО практики

\_\_\_\_\_  
(полное название организации; структурного подразделения)

Реквизиты договора  
о прохождении практической подготов-  
ке

(при проведении практической подготовки в организации)

Дата заключения Договора

« \_\_\_\_ » \_\_\_\_\_ 20 \_\_\_\_ г.

регистрационный номер № \_\_\_\_\_



МИНОБРНАУКИ РОССИИ



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

УТВЕРЖДАЮ

И.о. заведующего кафедрой

\_\_\_\_\_/\_\_\_\_\_/\_\_\_\_\_  
подпись И.О. Фамилия  
« \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

кафедра

**Комплексной защиты информации**  
(наименование)

направление подготовки

**10.03.01 Информационная безопасность**  
(код; наименование)

направленность (профиль)

**Организация и технология защиты информации**  
(наименование)

**РАБОЧИЙ ГРАФИК (ПЛАН) ПРОВЕДЕНИЯ ПРАКТИКИ**

Фамилия, Имя, Отчество обучающегося \_\_\_\_\_

курс

4

форма обучения

очная

вид практики

эксплуатационная

тип практики

стационарная

сроки практики

с « \_\_\_\_ » \_\_\_\_\_ 20\_\_ г. по « \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

МЕСТО практики

\_\_\_\_\_  
(полное название организации; структурного подразделения)

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

Дата заключения Договора  
« \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.  
регистрационный номер № \_\_\_\_\_

## Планируемые работы

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

**Рабочий график (план) составил:**

руководитель практики от РГГУ

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

**Согласовано (при проведении практики в профильной организации):**

руководитель практики от профильной организации

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

**С рабочим графиком (планом) ознакомлен:**

обучающийся

\_\_\_\_\_ «\_\_» \_\_\_\_\_ 20\_\_ г..  
(подпись)                      (И.О. Фамилия)                      (дата)

**ФОРМА ТИТУЛЬНОГО ЛИСТА ОТЧЁТА**

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

**ОТЧЁТ О ПРОХОЖДЕНИИ ПРАКТИКИ***Эксплуатационная практика*

Студента 3 курса

Фамилия Имя Отчество

направления подготовки 10.03.01 «Информационная безопасность»

(квалификация (степень) «бакалавр»)

профиль: «Организация и технология защиты информации»

Научный руководитель:

И. о. зав. кафедрой КЗИ, к.т.н.

\_\_\_\_\_ Д.А. Митюшин

\_\_\_\_\_ (оценка)

« \_\_\_\_ » \_\_\_\_\_ 2021 г.

Москва 20\_\_\_\_

**ОБРАЗЕЦ ОФОРМЛЕНИЯ ХАРАКТЕРИСТИКИ С МЕСТА ПРОХОЖДЕНИЯ ПРАКТИКИ**

**Характеристика<sup>1</sup>**

на студента/тку \_\_ курса \_\_\_\_\_ факультета  
Российского государственного гуманитарного университета  
\_\_\_\_\_ (ФИО)

\_\_\_\_\_ (ФИО) проходил/а производственную практику в \_\_\_\_\_  
\_\_\_\_\_ на должности \_\_\_\_\_.

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

За время прохождения практики \_\_\_\_\_ (ФИО) зарекомендовал/а себя как  
\_\_\_\_\_.

Оценка за прохождение практики – «\_\_\_\_\_».

Руководитель практики  
от организации

\_\_\_\_\_ (ФИО)

(дата)

(подпись)

\_\_\_\_\_

<sup>1</sup> Оформляется либо на бланке организации, либо заверяется печатью.

УТВЕРЖДЕНО  
Протокол заседания кафедры  
№ \_\_\_\_\_ от \_\_\_\_\_

### ЛИСТ ИЗМЕНЕНИЙ

в рабочей программе дисциплины Эксплуатационная практика  
по направлению подготовки 10.03.01 Информационная безопасность  
на 20\_\_/20\_\_ учебный год

1. В \_\_\_\_\_ вносятся следующие изменения:  
(элемент рабочей программы)

- 1.1. ....;
- 1.2. ....;
- ...
- 1.9. ....

2. В \_\_\_\_\_ вносятся следующие изменения:  
(элемент рабочей программы)

- 2.1. ....;
- 2.2. ....;
- ...
- 2.9. ....

3. В \_\_\_\_\_ вносятся следующие изменения:  
(элемент рабочей программы)

- 3.1. ....;
- 3.2. ....;
- ...
- 3.9. ....

Составитель  
дата

подпись

расшифровка подписи