ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА» (СПбГУТ)

Кафедра Защищенных систем связи
(полное наименование кафедры)

СПбГУТ))) Документ подписан простой электронной подписью
Сертификат: 00fd759708ffd39703
Владелец: Бачевский Сергей Викторович
Действителен с 15.03.2021 по 14.03.2026

УТВЕРЖДАЮ
Первый проректор - проректор по учебной работе
_____ Г.М. Машков
«02» 07 2021 г.

Регистрационный №_20.05/600-Д

ПРОГРАММА ПРАКТИКИ

Преддипломная практика
(наименование практики)

образовательная программа высшего образования

10.03.01 Информационная безопасность
(код и наименование направления подготовки / специальности)

бакалавр
(квалификация)

направленность (профиль) N 1 "Безопасность компьютерных систем" (по отрасли или в сфере профессиональной деятельности)
(направленность / профиль образовательной программы)

очная форма
(форма обучения)

Санкт-Петербург

Рабочая программа дисциплины составлена на основе требований Федерального государственного образовательного стандарта высшего образования по направлению (специальности) подготовки «10.03.01 Информационная безопасность», утвержденным приказом Министерства образования и науки Российской Федерации от 01.12.2016 № 1515, и в соответствии с рабочим учебным планом, утвержденным ректором университета.

1. Цели и задачи практики

Целью проведения практики «Преддипломная практика» является: закрепление и углубление теоретических знаний; формирование и развитие профессиональных знаний; приобретение практических навыков; формирование компетенций, а также приобретение опыта самостоятельной профессиональной и научной деятельности, необходимых для последующей профессиональной деятельности.

Эта цель достигается путем решения следующих(ей) задач(и):

- закрепление на практике знаний и умений, полученных в процессе теоретического обучения;
- развитие профессиональных навыков;
- ознакомление с общей характеристикой объекта практики и правилами техники безопасности;
- подбор необходимых материалов для выполнения выпускной квалификационной работы (или магистерской диссертации).

- Изучить документацию к средствам защиты, использующимся на территории РФ - Изучить основы организации систем контроля доступа и видеонаблюдения на режимном объекте - Изучить основные механизмы защиты в телекоммуникационных сетях

2. Место практики в структуре основной образовательной программы

«Преддипломная практика» Б2.В.02.02(Пд) входит в блок 2 учебного плана, который относится к вариативной части, и является обязательной составной частью образовательной программы по направлению «10.03.01 Информационная безопасность».

«Преддипломная практика» опирается на знания и практические навыки полученные при изучении дисциплин и прохождении всех типов практик. «Преддипломная практика» является завершающей в процессе обучения и предшествует выполнению выпускной квалификационной работы.

3. Вид, тип, способ, форма проведения практики

Вид практики – производственная

Тип практики – «Преддипломная практика»

Способ проведения – стационарная; выездная

Форма проведения – дискретно по видам и по периодам проведения практик

Стационарная практика может проводиться в структурных подразделениях университета.

4. Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения образовательной программы

В процессе прохождения практики «Преддипломная практика» студент формирует и демонстрирует следующие компетенции:

Компетенции, установленные ФГОС ВО

Таблица 1

№ п/п	Код компетенции	Наименование компетенции
1	ОПК-4	способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации
2	ОПК-5	способностью использовать нормативные правовые акты в профессиональной деятельности
3	ОПК-7	способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты
4	ПК-1	способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
5	ПК-2	способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач
6	ПК-3	способностью администрировать подсистемы информационной безопасности объекта защиты
7	ПК-4	способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты
8	ПК-5	способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации
9	ПК-6	способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации
10	ПК-7	способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений
11	ПК-8	способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов
12	ПК-9	способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности
13	ПК-10	способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности
14	ПК-11	способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов
15	ПК-12	способностью принимать участие в проведении экспериментальных исследований системы защиты информации

Планируемые результаты обучения

Таблица 2

Навыки компетенции ОПК-4

знать	базовые понятия информации и информационных технологий; структуру и принципы функционирования языка С++; структуру и принципы функционирования языка С++ (ОПК-4);;
уметь	использовать основные методы программирования на языке С++ для разработки защищенных приложений; использовать основные методы программирования на языке С++ для разработки защищенных приложений (ОПК-4);; применять информационные технологии обработки информации и данных;
владеть	навыками разработки программного обеспеченья средствами языка С++ (ОПК-4);; навыками разработки программного обеспеченья средствами языка С++; навыки решения профессиональных задач с использованием компьютерных средств и ИТ;

Навыки компетенции ОПК-5

знать	Нормативно-правовую базу РФ в сфере обеспечения информационной безопасности; теоретические основы права, основные положения институтов информационного права, отраженных в нормативно-правовых актах; (ОПК-5, ПК-8, ПК-10);; теоретические основы права, основные положения институтов информационного права, отраженных в нормативно-правовых актах; (ОПК-5; ПК-8;);;
уметь	анализировать конкретные социально-экономические и социально-правовые ситуации в условиях рыночной экономики, быстро меняющейся технико-экономической конъюктуры и конкурентной среды отрасли (ПК-10);; Применять нормативно-правовую базу РФ в сфере обеспечения информационной безопасности; разрабатывать меры по улучшению правовой ситуации;
владеть	Владеть орматично-правовую базу РФ в сфере обеспечения информационной безопасности; методами управления и регулирования правовых отношений отрасли инфокоммуникаций в рыночной среде; методами управления и регулирования правовых отношений отрасли инфокоммуникаций в рыночной среде (ПК-10);

Навыки компетенции ОПК-7

знать	Архитектуру микропроцессоров 8080 и 8085;Классификацию регистров памяти и методов ввода-вывода ;Структурные схемы программно-аппаратных средств защиты информации на основе микропроцессоров 8086/8088 и сопроцессоров 8087 ;; информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; Нормативно правовые акты, законы РФ, организаций регламентирующих защиту информации, коммерческой тайны; • виды и основные характеристики инженерно-технических средств защиты объектов инфокоммуникаций ;• основные источники и носители информации объектов инфокоммуникаций ; • демаскирующие признаки объектов защиты объектов инфокоммуникаций ; • угрозы безопасности инженерно-технической защиты объектов инфокоммуникаций ; • принципы добывания информации; • возможности технических каналов утечки информации объектов инфокоммуникаций и методы их оценки ; • методы и способы защиты объектов инфоком; • Способы организации и поддержки комплекса мер по информационной безопасности, управления процессом их реализации;
уметь	анализировать и совершенствовать уровень защиты информации в документообороте организации; определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; организовать рабочие места, их техническое оснащение, размещение сооружений, средств и оборудования инженерной защиты объектов инфокоммуникаций ;составлять нормативную документацию (инструкции) по эксплуатационно-техническому обслуживанию оборудования систем инженерной защиты объектов инфокоммуникаций ;организовать и осуществить проверку технического состояния и оценить остаток ресурса сооружений, оборудования и средств инженерной защиты объектов инфокоммуникаций, применить современные методы их обслужи; применять на практике полученные теоретические знания, для проведения оценок используемых систем защиты информации; работать со средой разработки современных программно-аппаратных средств микроконтроллерной техники;; Программно реализовать алгоритмы безопасности;

владеть	навыками составления пакетов документации для контрольно-надзорных органов в области документооборота организации; основами методов построения программно-аппаратных средств защиты информации на основе микроконтроллерной техники ;- основами программирования на языках C/C++ для создания приложений для обработки информации на микроконтроллерах ;основами программирования на языке Ассемблер для создания приложений для обработки информации на микроконтроллерах; принципами и навыками инструментальных измерений, используемых в области инженерной защиты объектов инфокоммуникаций; способностями осуществить приемку, освоение и эксплуатацию вводимого оборудования инженерно-технической защиты объектов инфокоммуникаций в соответствии с действующими нормативами ;способностями осуществить монтаж, наладку, настройку, испытания и сдачу в эксплуатацию сооружений, средств и оборудования систем инженерной защиты объектов инфокоммуникаций ;способностями к разработке проектной; способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; • Методами организации защиты объекта от внешних угроз и технологиями защиты информации;

Навыки компетенции ПК-1

знать	архитектуру Cisco Enterprise; архитектуру беспроводной сети LAN; архитектуру локальных вычислительных сетей, сетевые протоколы стека TCP/IP; динамический протокол маршрутизации EIGRP (ПК-1); компоненты решений унифицированных взаимодействий Cisco; компоненты решений унифицированных взаимодействий Cisco (ПК-1); Методы разработки мобильных приложений;; основные методы защиты сетевой инфраструктуры на базе коммутаторов и маршрутизаторов; основы коммутации; стек протоколов IPSEC (ПК-1, ПС-10);
уметь	настраивать виртуальные локальные сети. Маршрутизацию между виртуальными локальными сетями; настраивать протокол динамической маршрутизации OSPFдля нескольких областей (ПК-1); настраивать трансляцию сетевых адресов; описывать существующую компьютерную сеть, описывать требования (влияние используемых приложений, требования пользователей, технические параметры и др.); определять архитектуру WLAN исходя из сопутствующей сетевой инфрастуктуры; основные принципы адресации и коммутации в корпоративной сети (ПК-1). - определять структуру сообщений сигнализации и медиапотока (ПК-1);; основные принципы адресации и коммутации в корпоративной сети (ПК-1).- определять структуру сообщений сигнализации и медиапотока (ПК-1);; разрабатывать комплексную политику сетевой безопасности (ПК-1, ПС-10); Разрабатывать мобильные приложения;; эффективно использовать средства защиты периметра сети с помощью маршрутизаторов;

владеть	навыками мониторинга компьютерной сети; навыками настройки адресации в сети; навыками настройки беспроводного маршрутизатора CiscoLinkSys (ПС-9).; навыками настройки статических (site-to-site) VPN соединений (ПС-8); навыками настройки статических маршрутов; навыками поддержки технологии обеспечения удалённого доступа (SSL VPN, Easy VPN) с помощью маршрутизаторов; Навыками разработки защищенных мобильных приложений.; навыками решения задачи конфигурирования пользователей и пользовательских устройств в решениях Cisco Unified Communications Manager и Cisco Unified Communications Manager Express; навыками решения задачи конфигурирования пользователей и пользовательских устройств в решениях Cisco Unified Communications Manager и Cisco Unified Communications Manager Express (ПК-1); принципы базовой настройки и базовые сервисы;;

Навыки компетенции ПК-2

знать	алгоритмы применения аппаратно-программных средств; основные виды и наиболее известные примеры программных уязвимостей; основные виды и наиболее известные примеры программных уязвимостей (ПК-2);; структуру и принципы функционирования языка Ассемблер; технические вопросы, связанные с защитой от вредоносного программного обеспечения (ПК-2);;
уметь	выполнять Машинно-независимая оптимизации, Распараллеливание, Обфускации, модификации ПО (ПК-2); использовать основные методы программирования на языке Ассемблер для разработки приложений; применять программно-аппаратные средства для решения поставленных задач; проводить экспертизу качества и надежности программных и программно-аппаратных средств обеспечения информационной безопасности; проводить экспертизу качества и надежности программных и программно-аппаратных средств обеспечения информационной безопасности; (ПК-2); работать с антивирусным программным обеспечением(ПК-2);;
владеть	владеть навыками работы с программами и данными; вопросами навыками работы с современными дизассемблерами и отладчиками; вопросами навыками работы с современными дизассемблерами и отладчиками (ПС-15);; навыками работы с программами и данными; навыками разработки программного обеспечения средствами языка Ассемблер; умением писать простые программы на языках C++, java (ПК-2);;

Навыки компетенции ПК-3

знать	Основные методы администрирования ОС GNULinux.; стандартные средства операционных систем по обеспечению информационной безопасности;
уметь	настраивать политики информационной безопасности операционных систем; Организовывать аудит системы.;
владеть	алгоритмами обработки сетевого трафика стандартами утилитами ОС; вопросами администрирования ОС GNULinux и MS Windows Server; Встроенным набором утилит для управления системой.; Организовывать мониторинг Security-Enhanced Linux и управление моделью безопасности в ОС;

Навыки компетенции ПК-4

знать	Нормативно-правовую документацию по защите информации; основные методы защиты сетевой инфраструктуры на базе коммутаторов и маршрутизаторов; принципы организации корпоративной связи WAN;
уметь	внедрять протокол IPv6; работать с антивирусным программным обеспечением;
владеть	основами методов защиты информации в компьютерных сетях; Особенностями настройки антивирусного программного обеспечения;

Навыки компетенции ПК-5

знать	виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия;
уметь	Проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности;
владеть	навыками реализации методов и путей реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия;

Навыки компетенции ПК-6

знать	возможности технических каналов утечки информации объектов инфокоммуникаций и методы их оценки;
уметь	составить заявку на оборудование, измерительные устройства и запасные части, подготовить техническую документацию на ремонт и восстановление работоспособности оборудования, средств, систем инженерной;
владеть	принципами и навыками инструментальных измерений, используемых в области инженерной защиты объектов инфокоммуникаций;

Навыки компетенции ПК-7

знать	архитектуру построения дата-центров (ПК-7); набор исходных данных для проектирования подсистем и средств обеспечения информационной безопасности;
уметь	конфигурировать устройства, обеспечивающие работу ЦОД (ПК-7); проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности; проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных; эффективно использовать средства защиты периметра сети с помощью маршрутизаторов;
владеть	навыками настройки политик безопасности в ЦОД (ПК-7); навыками проведения технико-экономического обоснования соответствующих проектных решений;

Навыки компетенции ПК-8

знать	основные понятия, связанные с лицензированием программного обеспечения; принципы проведения оценки рисков и аудита ИБ; Содержание действующих нормативных и методических документов по оформлению рабочей технической документации; формирование фундамента подготовки будущих специалистов в области инфокоммуникаций;

уметь	Оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов; пользоваться технической документации при лицензировании ПО;
владеть	Знаниями действующих и методических документов и навыками по оформлению рабочей технической документации; основными критериями использования нормативных правовых актов при лицензировании ПО;

Навыки компетенции ПК-9

знать	Нормативно-правовую базу РФ в сфере обеспечения информационной безопасности;
уметь	осуществлять подбор, изучение и обобщение научно-технической литературы; Применять знания о правовом обеспечении защиты информации;
владеть	Методами применения нормативно-правовых актов РФ в отношении защиты информации;

Навыки компетенции ПК-10

знать	Знания о правовом обеспечении защиты информации; структуру государственной системы защиты информации;
уметь	анализировать конкретные социально-экономические и социально-правовые ситуации в условиях рыночной экономики, быстро меняющейся технико-экономической конъюктуры и конкурентной среды отрасли (ПК-10);; Применять знания о правовом обеспечении защиты информации; применять современные теоретические и экспериментальные методы исследования с целью создания новых перспективных средств инженерно-технической защиты объектов инфокоммуникаций; организовывать и проводить их испытания с целью оценки соответствия требованиям технических регламентов, международных и национальных стандартов и иных нормативных документов;
владеть	Знаниями о правовом обеспечении защиты информации;

Навыки компетенции ПК-11

знать	Стандартные средства операционных систем по обеспечению информационной безопасности;
уметь	Настраивать политики информационной безопасности операционных систем специального назначения;
владеть	вопросами администрирования ОС GNULinux;

Навыки компетенции ПК-12

знать	Методы и средства защиты беспроводных сетей; Методы и средства защиты электронного документооборота; методы проведения экспериментальных исследований системы защиты информации;
уметь	Защищать электронный документооборот; прооводить экспериментальные исследования; эффективно использовать методы защиты мобильных приложений; Эффективно использовать средства защиты периметра сети с помощью маршрутизаторов;
владеть	Методами защиты электронного документооборота; Методами и средствами для защиты электронного документооборота; Методами и средствами защиты беспроводных сетей; Навыками настройки статических маршрутов; способностью принимать участие в проведении экспериментальных исследований системы защиты информации;

5. Объем практики и виды учебной работы

Очная форма обучения

Таблица 3

Вид учебной работы		Всего часов	Семестры
			8
Общая трудоемкость	9 ЗЕТ	324	324
Контактная работа с обучающимися			-
Работа под руководством преподавателя		234	234
Анализ данных, подготовка отчета, зачет		90	90.00
Самостоятельная работа обучающихся (СРС)			-
Вид промежуточной аттестации			Зачет

6. Содержание практики

6.1. Содержание разделов дисциплины.

Таблица 4

№ п/п	Наименование раздела (темы) дисциплины	Содержание раздела	№ семестра		
			очная	очно-заочная	заочная
1	Раздел 1. Согласование темы индивидуального задания	Выбор и согласование темы с научным руководителем	8		
2	Раздел 2. Составление индивидуального плана работы студента	определение и согласование индивидуального плана работы	8		
3	Раздел 3. Выполнение индивидуального задания	получение и выполнение индивидуального задания	8		
4	Раздел 4. Подготовка отчета	оформление и подготовка работы	8		
5	Раздел 5. Защита отчета	выступление и защита работы	8		

6.2. Междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами.

«Преддипломная практика» является базой для написания бакалаврской работа

7. Методические рекомендации по организации проведения практики и формы отчетности

Организация практики на всех этапах обучения в вузе направлена на обеспечение непрерывности и последовательности овладения обучающимися профессиональной деятельностью и приобретения ими компетенций в соответствии с требованиями образовательных стандартов к уровню подготовки выпускников.

Перед началом прохождения практики студент должен пройти инструктаж о

правилах поведения и технике безопасности на рабочем месте, получить индивидуальное задание и ознакомиться с соответствующими должностными инструкциями и регламентными документами.

После получения индивидуального задания и прохождения необходимой теоретической подготовки, студент составляет календарный план выполнения задания и согласовывает его с руководителем практики от организации на которой он проходит практику.

По итогам практики руководитель от организации выставляет оценку, которая должна учитывать выполнение календарного графика практики, качество выполнения индивидуального задания, отчета о прохождении практики, профессиональные навыки студента, полученные в ходе прохождения практики.

Отчет о прохождении практики и заполненный индивидуальный бланк задания сдается руководителю практики от университета. В ходе собеседования руководитель практики анализирует данные отчета, оценку и отзыв руководителя практики от организации при необходимости задает студенту дополнительные вопросы и выставляет итоговую оценку.

Методическая и другая литература, необходимая для обеспечения самостоятельной работы студентов на практике, рекомендуется руководителем практики в соответствии с индивидуальным заданием, выданным студенту.

Студент, не прошедший практику по неуважительной причине в сроки, установленные учебным планом, или получивший по результатам прохождения практики неудовлетворительную оценку, может быть отчислен из СПбГУТ, как имеющий академическую задолженность.

8. Учебно-методическое обеспечение практики

8.1. Основная литература:

1. Колесов, Ю.
   Моделирование систем. Объектно-ориентированный подход : [Электронный ресурс] / Ю. Колесов, Ю. Сениченков. - Санкт-Петербург : БХВ-Петербург, 2012. - 192 с. : ил. - URL: http://ibooks.ru/reading.php?productid=24857. - ISBN 978-5-94157-579-3 : Б. ц.
2. Губарев, В. В.
   Квалификационные исследовательские работы : [Электронный ресурс] : учеб. пособие / В. В. Губарев, О. В. Казанская. - 2-е изд., испр. - Новосибирск : НГТУ, 2014. - 80 с. - URL: https://e.lanbook.com/book/118102. - ISBN 978-5-7782-2472-8 : Б. ц. Книга из коллекции НГТУ - Инженерно-технические науки. Утверждено Редакционно-издательским советом университета в качестве учебного пособия

8.2. Дополнительная литература:

1. Шелухин, О. И.
   Моделирование информационных систем. Учебное пособие для вузов : [Электронный ресурс] / О. И. Шелухин. - М. : Горячая линия-Телеком, 2012. - 516 с. : ил. - URL: http://ibooks.ru/reading.php?productid=334050. - ISBN 978-5-9912-

0193-3 : Б. ц.
2. Сафин, Р. Г.
Основы научных исследований. Организация и планирование эксперимента : [Электронный ресурс] : учебное пособие / Р. Г. Сафин, А. И. Иванов, Н. Ф. Тимербаев. - Казань : КНИТУ, 2013. - 156 с. - URL: http://e.lanbook.com/books/element.php?pl1_id=73344. - ISBN 978-5-7882-1414-2 : Б. ц. Книга из коллекции КНИТУ - Лесное хозяйство и лесоинженерное дело

9. Материально-техническое обеспечение практики

Таблица 5

№ п/п	Наименование специализированных аудиторий и лабораторий	Наименование оборудования
1	Аудитория для самостоятельной работы	Персональные компьютеры
2	Читальный зал	Персональные компьютеры

Рабочее место: Оборудование, используемое при выполнении индивидуального задания непосредственно в организации.

10. Ресурсы информационно-телекоммуникационной сети «Интернет»

10.1. Информационно-справочные системы:

- ЭБС iBooks (https://ibooks.ru)
- ЭБС Лань (https://e.lanbook.com/)
- ЭБС СПбГУТ (http://lib.spbgut.ru)

10.2. Ресурсы информационно-телекоммуникационной сети «Интернет»

При изучении дисциплины ресурсы информационно-телекоммуникационной сети «Интернет» не задействуются

11. Фонд оценочных средств для проведения промежуточной аттестации обучающихся

Фонд оценочных средств разрабатывается в соответствии с Методическими рекомендациями по формированию ФОС и приказом Минобрнауки России от 5 апреля 2017г. № 301, г. Москва "Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры" и является приложением к рабочей программе дисциплины.

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по **практике** включает в себя:

- перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы;
- описание показателей и критериев оценивания компетенций на различных этапах

их формирования, описание шкал оценивания;
- типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы;
- методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Для каждого результата обучения по дисциплине определяются показатели и критерии оценки сформированности компетенций на различных этапах их формирования, шкалы и процедуры оценивания.