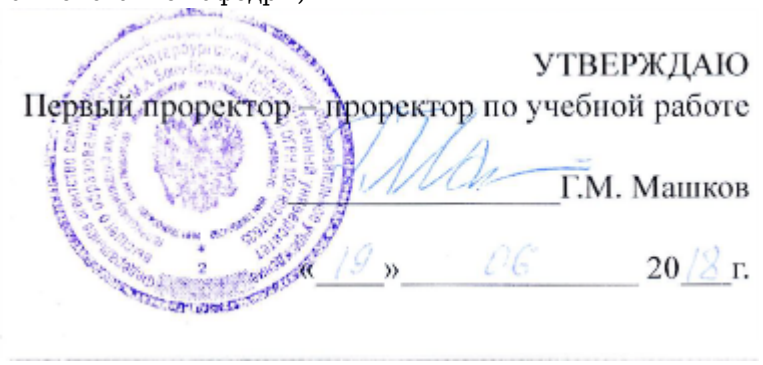
ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

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)



Регистрационный №_18.05/2424-Д

ПРОГРАММА ПРАКТИКИ

Практика по получению профессиональных умений и опыта профессиональной деятельности
(наименование практики)

образовательная программа высшего образования

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

магистр
(квалификация)

Безопасность компьютерных систем
(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 «10.04.01 Информационная безопасность», утвержденным приказом Министерства образования и науки Российской Федерации от 01.12.2016 № 1513, и в соответствии с рабочим учебным планом, утвержденным ректором университета.

1. Цели и задачи практики

Целью проведения практики «Практика по получению профессиональных умений и опыта профессиональной деятельности» 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;

2. Место практики в структуре основной образовательной программы

«Практика по получению профессиональных умений и опыта профессиональной деятельности» Б2.В.01.02(П) входит в блок 2 учебного плана, который относится к вариативной части, и является обязательной составной частью образовательной программы по направлению «10.04.01 Информационная безопасность».

«Практика по получению профессиональных умений и опыта профессиональной деятельности» опирается на знания полученные при изучении предшествующих дисциплин, а также на знания и практические навыки, полученные при прохождении практик(и) «Научно-исследовательская работа».

3. Вид, тип, способ, форма проведения практики

Вид практики – производственная

Тип практики – «Практика по получению профессиональных умений и опыта профессиональной деятельности»

Способ проведения – стационарная; выездная

Форма проведения – непрерывно

Стационарная практика может проводиться в структурных подразделениях университета.

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

В процессе прохождения практики «Практика по получению профессиональных умений и опыта профессиональной деятельности» студент формирует и демонстрирует следующие компетенции:

Компетенции, установленные ФГОС ВО

Таблица 1

№ п/п	Код компетенции	Наименование компетенции

1	ОПК-2	способностью к самостоятельному обучению и применению новых методов исследования профессиональной деятельности
2	ПК-1	способностью анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты
3	ПК-2	способностью разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности
4	ПК-3	способностью проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов
5	ПК-4	способностью разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности
6	ПК-5	способностью анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества
7	ПК-6	способностью осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок
8	ПК-7	способностью проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента
9	ПК-8	способностью обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи
10	ПК-9	способностью проводить аудит информационной безопасности информационных систем и объектов информатизации
11	ПК-10	способностью проводить аттестацию объектов информатизации по требованиям безопасности информации
12	ПК-12	способностью организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения
13	ПК-13	способностью организовать управление информационной безопасностью
14	ПК-14	способностью организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России
15	ПК-15	способностью организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности
16	ПК-16	способностью разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности

Планируемые результаты обучения

Таблица 2

Навыки компетенции ОПК-2

знать	актуальную и полную информацию о компонентах и сборке компьютеров, ноутбуках и мобильных устройствах, операционных системах и прикладном ПО, малых сетях и беспроводной связи, принтерах и сканерах, технике безопасности и информационной безопасности, охране окружающей среды и навыках общения.; современные методы научных исследований и информационно-коммуникационных технологий в области организации информационной безопасности социально-экономических информационных систем;
уметь	самостоятельно находить и применять новые методы исследования профессиональной деятельности;
владеть	методами исследования профессиональной деятельности;

Навыки компетенции ПК-1

знать	как прогнозировать эффективность функционирования при больших объемах данных, оценивать затраты и риски объектов защиты больших данных; основные методики оценки уровня информационной безопасности организации и примеры их использования;
уметь	работать с основными программами, позволяющими реализовывать аудит систем ИБ и - работать с государственными и международными стандартами, регулирующих деятельность; формировать политику безопасности объектов защиты больших данных и прогнозировать эффективность функционирования при больших объемах данных;
владеть	способностью анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты;

Навыки компетенции ПК-2

знать	основы виртуализации OpenStack; основы построения мобильных приложений; систему подбора и обоснования технологий обеспечения информационной безопасности в зависимости от характера объекта информатизации; структуру байт-кода;
уметь	использовать в разрабатываемых программах механизмы наследования, полиморфизма, обработки исключений; конфигурировать системы предотвращения вторжений; применять современные технологии защиты объектов информатизации современными технологиями для формирования проектных решений защите объектов информатизации;
владеть	методами разработки средств обеспечения информационной безопасности; навыками настройки IPS систем с открытым исходным кодом – Snort; системой обеспечение уровня безопасности предприятия;

Навыки компетенции ПК-3

знать	принципы правового регулирования отношений в сфере информации;
уметь	проводить мониторинг защищенности компьютерных сетей и систем;
владеть	способностью проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов;

Навыки компетенции ПК-4

знать	Алгоритмы создания программ; законодательную основу и ограничения, регулирующие санкционированное проведение аудита и теста на проникновение; перечень сведений, составляющих государственную тайну в РФ; • разрабатывать технические решения по защите от несанкционированного доступа межсетевого взаимодействия инфокоммуникационных систем; • разрабатывать технические решения по защите компьютерных ресурсов от несанкционированного доступа на уровне серверов и рабочих станций в закрытых и открытых контурах локальной вычислительной сети инфокоммуникационной системы; • разрабатывать технические решения по реализации подсистемы аутентификации и идентификации в закрытых и открытых контурах локальной вычислительной с;
уметь	готовить необходимую инфраструктуру для проведения теста на проникновение; Проводить испытания средств и систем обеспечения информационной безопасности; проводить мониторинг защищенности компьютерных сетей и систем; разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности;
владеть	методами проведения аудита безопасности сетей; методиками испытаний средств и систем обеспечения информационной безопасности; Навыки настройки систем обеспечения информационной безопасности; принципами разработки программ и методик испытаний средств и систем обеспечения информационной безопасности; способностью разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности;

Навыки компетенции ПК-5

знать	возможности обеспечения защиты оборудования от ЭМИ, КЗ, скачков напряжения; технологию организации обеспечения информационной безопасности;
уметь	выбирать способы решения прикладных проблем информационной безопасности в условиях становления современного информационного общества; обеспечить защиту оборудования от ЭМИ, КЗ, скачков напряжения;
владеть	методами, обеспечивающими защиту оборудования от ЭМИ, КЗ, скачков напряжения; основными терминами и понятиями в области информационной безопасности;

Навыки компетенции ПК-6

знать	методы сбора, обработки, анализа и систематизации научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок; Особый порядок допуска к государственной тайне.;
уметь	проводить мониторинг защищенности компьютерных сетей и систем; работать самостоятельно и в коллективе для решения производственных задач и повышения собственной квалификации;
владеть	навыками работы самостоятельно и в коллективе для решения производственных задач и повышения собственной квалификации; способностью осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок;

Навыки компетенции ПК-7

знать	классификацию основных типов уязвимостей в системах; основные элементы информационной безопасности; физические и математические методы экспериментального исследования защищенности объектов с применением соответствующих технических и программных средств обработки результатов эксперимента;
уметь	проводить аудит систем безопасности в корпоративных системах; проводить расследование инцидентов ИБ в различных файловых системах; прогнозировать основные опасности и угрозы, возникающие в процессе информационного взаимодействия;
владеть	методами моделирования систем информационной безопасности; навыками написания отчетов по форензике; навыками обнаружения уязвимостей в корпоративных сетях;

Навыки компетенции ПК-8

знать	обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи; Основания для отказа должностному лицу или гражданину в допуске к государственной тайне;
уметь	проводить мониторинг защищенности компьютерных сетей и систем; совершить сборку, ремонт, настройку ПК, ноутбуков и мобильных устройств. Установить и настроить ОС и прикладное ПО;
владеть	базовыми знаниями по настройки сетей, установке и настройке компьютерной техники, сборка компьютерной техники, восстановление данных, знания операционных систем UNIX подобных и Windows подобных.; способностью обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи;

Навыки компетенции ПК-9

знать	как проводить проверку информационной безопасности больших данных; классификацию основных типов уязвимостей в системах;
уметь	проводить аудит информационной безопасности информационных систем с большим объемом данных; проводить аудит систем безопасности в корпоративных сетях;
владеть	методами проведения аудита безопасности систем; способностью проводить аудит информационной безопасности информационных систем и объектов информатизации;

Навыки компетенции ПК-10

знать	основные положения Устава и Конвенции Международного союза электросвязи;
уметь	формировать политику безопасности объектов защиты;
владеть	способностью проводить аттестацию объектов информатизации по требованиям безопасности информации;

Навыки компетенции ПК-12

знать	принципы работы с большими данными, основные понятия, касающиеся технологий обеспечения информационной безопасности больших данных;

уметь	анализировать направления развития информационных (телекоммуникационных) технологий связанных с большими данными, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты, проводить мониторинг защищенности компьютерных сетей и систем;
владеть	способностью организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения;

Навыки компетенции ПК-13

знать	организацию управления ИБ;
уметь	производить организацию по управлению ИБ;
владеть	способностью организовать управление информационной безопасностью;

Навыки компетенции ПК-14

знать	обязанности организатора распространения информации в сети "Интернет"; принципы работы с большими данными, основные понятия, касающиеся технологий обеспечения информационной безопасности больших; принципы работы с большими данными, основные понятия, касающиеся технологий обеспечения информационной безопасности больших данных;
уметь	анализировать направления развития информационных (телекоммуникационных) технологий связанных с большими данными, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты, проводить мониторинг защищенности компьютерных сетей и систем; организовывать работу по созданию или модернизации систем и средств обеспечения ИБ в соответствии с правовыми нормами; проводить мониторинг защищенности компьютерных сетей и систем;
владеть	способностью организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России;

Навыки компетенции ПК-15

знать	виды информации в зависимости от категории доступа и в зависимости от порядка ее предоставления или распространения;
уметь	различать виды информации, причиняющие вред здоровью и (или) развитию детей.;
владеть	проводить мониторинг защищенности компьютерных сетей и систем;

Навыки компетенции ПК-16

знать	разработку проектов, бизнес-планов, технической и эксплуатационной документации на системы, средства обеспечения ИБ; специфику технологий обеспечения информационной безопасности объектов защиты;
уметь	разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения ИБ; формировать требования к технологиям обеспечения информационной безопасности объектов защиты;

владеть	приемами и методами анализа информационной системы для выбора технологий обеспечения информационной безопасности объекта информатизации; способностью разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности;

Дополнительные компетенции

Таблица 3

№ п/п	Код компетенции	Наименование компетенции
1	ПС-1	Проведение контрольных проверок работоспособности программно-аппаратных средств защиты информации
2	ПС-2	Проведение контрольных проверок эффективности применяемых программно-аппаратных средств защиты информации
3	ПС-3	Формирование политик информационной безопасности
4	ПС-4	Разработка требований по защите компьютерных сетей и систем
5	ПС-5	Разработка средств защиты информации
6	ПС-6	Разработка требований по защите информации беспроводных и мобильных компьютерных сетей
7	ПС-7	Оценка рисков угроз и соответствия требованиям нормативных документов информационной безопасности
8	ПС-8	Проведение анализа безопасности компьютерных систем
9	ПС-9	Проведение сертификации программно-аппаратных средств защиты информации
10	ПС-10	Проведение экспериментальных исследований уровней защищенности компьютерных сетей и систем

Планируемые результаты обучения

Таблица 4

Навыки компетенции ПС-1

знать	методы контрольных проверок работоспособности программно-аппаратных средств защиты информации; современные методы обеспечения целостности и защиты информации;
уметь	выбирать соответствующие организационные и программно-аппаратные средства для организации систем информационной защиты; совершить базовую настройку локальной сети и беспроводной локальной сети.;
владеть	защищать папки и файлы в ОС Windows; методами контрольных проверок работоспособности программно-аппаратных средств защиты информации;

Навыки компетенции ПС-2

знать	методы и средства обеспечения информационной безопасности компьютерных систем; поведение вредоносного ПО;
уметь	осуществлять защиту офисных электронных документов; предотвратить атаку на корпоративную сеть;
владеть	базовыми навыками защиты от вирусных атак; навыками оптимизации механизмов информационной безопасности;

Навыки компетенции ПС-3

знать	актуальную и полную информацию о формировании политик информационной безопасности; Формирование политик информационной безопасности; • основные этапы построения политики информационной безопасности информационных систем; • основные приоритеты информационной безопасности; • модели нарушителя и угроз в закрытых и открытых контурах локальной вычислительной сети инфокоммуникационных систем; • требования, предъявляемые к безопасности информации в закрытых и открытых контурах локальной вычислительной сети инфокоммуникационной системы;
уметь	разрабатывать нормы и политики ИБ; разрабатывать технические решения по защите от несанкционированного доступа межсетевого взаимодействия инфокоммуникационных систем; • разрабатывать технические решения по защите компьютерных ресурсов от несанкционированного доступа на уровне серверов и рабочих станций в закрытых и открытых контурах локальной вычислительной сети инфокоммуникационной системы; • разрабатывать технические решения по реализации подсистемы аутентификации и идентификации в закрытых и открытых контурах локальной вычислительной сет; установить и настроить, оказать помощь в эксплуатации периферийных устройств, оргтехники и техники специального назначения;
владеть	методологией построения политики информационной безопасности инфокоммуникационных систем; навыками и методами формирования политик информационной безопасности; умением формировать и создавать политики ИБ;

Навыки компетенции ПС-4

знать	основы виртуализации VMware; разработку требований по защите компьютерных сетей и систем; требования, установленные ФСТЭК;
уметь	использовать механизм обеспечения информационной безопасности, как алгоритмы шифрования; настраивать ESXi; разрабатывать требования по защите компьютерных сетей и систем;
владеть	методами формулировки требований к защите при разработке приложений; навыками работы с гипервизорами; разработкой требований по защите компьютерных сетей и систем;

Навыки компетенции ПС-5

знать	алгоритмы шифрования, аутентификации, цифровой подписи, цифровых сертификатов; основы облачных вычислений;
уметь	использовать механизм обеспечения информационной безопасности, как цифровые сертификаты; конфигурировать системы предотвращения аномалий;
владеть	навыками обеспечения защиты данных; средствами создания интерфейса;

Навыки компетенции ПС-6

знать	актуальную и полную информацию по разработка требований по защите информации беспроводных и мобильных компьютерных сетей; основную структуру кода защищённого приложения;
уметь	создавать исполняемые файлы из исходного кода; создавать резервные копии данных, восстановление утраченных;

владеть	навыками по разработке требований по защите информации беспроводных и мобильных компьютерных сетей;

Навыки компетенции ПС-7

знать	как производить оценку рисков угроз, а также проверять соответствия требованиям нормативных документов ИБ;
уметь	давать оценку рискам угроз и оценивать соответствия требованиям нормативных документов ИБ;
владеть	оценкой рисков угроз и соответствия требованиям нормативных документов информационной безопасности;

Навыки компетенции ПС-8

знать	актуальную и полную информацию по проведению анализа безопасности компьютерных систем; Анализы безопасности компьютерных систем;
уметь	Анализировать безопасность компьютерных систем; провести анализ безопасности компьютерных систем;
владеть	Алгоритмами анализа безопасности компьютерных систем; методами и навыками обеспечения анализа безопасности компьютерных систем; навыками проведения аудита безопасности информационных систем;

Навыки компетенции ПС-9

знать	программно-аппаратные средства защиты информации;
уметь	проводить сертификации;
владеть	владеть знаниями в сфере защиты информации;

Навыки компетенции ПС-10

знать	Правовые основы деятельности связи в РФ;
уметь	анализировать направления развития информационных (телекоммуникационных) технологий связанных с большими данными;
владеть	навыками работы с большими данными;

5. Объем практики и виды учебной работы

Очная форма обучения

Таблица 5

Вид учебной работы		**Всего часов**	**Семестры**	
			2	4
Общая трудоемкость	15 ЗЕТ	540	216	324
Контактная работа с обучающимися			-	-
Работа под руководством преподавателя		390	156	234
Промежуточная аттестация		150	60.00	90.00
Самостоятельная работа обучающихся (СРС)			-	-
Вид промежуточной аттестации			Зачет	Зачет

6. Содержание практики

6.1. Содержание разделов дисциплины.

Таблица 6

№ 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			
2	Раздел 2. Составление индивидуального плана работы студента	определение и согласование индивидуального плана работы			
3	Раздел 3. Выполнение индивидуального задания	получение и выполнение индивидуального задания			
4	Раздел 4. Подготовка отчета	оформление и подготовка работы			
5	Раздел 5. Защита отчета	выступление и защита работы			

6.2. Междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами.

Таблица 7

№ п/п	Наименование обеспечиваемых (последующих) дисциплин

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. Вольфсон, Михаил Борисович. Организация электронного бизнеса [Электронный ресурс] : учеб. пособие / М. Б. Вольфсон ; рец.: Б. А. Колтынюк, Ю. П. Левчук ; Федер. агентство связи, Федер. гос. образовательное бюдж. учреждение высш. проф. образования "С.-Петерб. гос. ун-т телекоммуникаций им. проф. М. А. Бонч-Бруевича". - СПб. : СПбГУТ, 2014. - 259 с. : ил. - ISBN 978-5-89160-111-6 (в обл.) : 1581.81 р.
2. Акимова, Е. В. Информационные системы и технологии в экономике и управлении. Экономические информационные системы [Электронный ресурс] : учебное пособие / Акимова Е. В. - Саратов : Вузовское образование, 2016. - 172 с. - Б. ц. Книга находится в Премиум-версии ЭБС IPRbooks.
3. Данилин, А. Архитектура предприятия [Электронный ресурс] : учебное пособие / Данилин А. - Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. - 439 с. - ISBN 5-9556-0045-0 : Б. ц. Книга находится в Премиум-версии ЭБС IPRbooks.
4. Блинов, А. О. Реинжиниринг бизнес-процессов [Электронный ресурс] : учебное пособие для студентов вузов, обучающихся по специальностям экономики и управления / Блинов А. О. - Москва : ЮНИТИ-ДАНА, 2015. - 343 с. - ISBN 978-5-238-01823-2 : Б. ц. Книга находится в Премиум-версии ЭБС IPRbooks.
5. Арзуманян, Максим Юрьевич. Архитектура предприятия [Электронный ресурс] : учебное пособие / М. Ю. Арзуманян ; рец.: Д. В. Кудрявцев, И. Б. Щербаков ; Федеральное агентство связи, Федеральное государственное бюджетное образовательное учреждение высшего образования "Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича". - СПб. : СПбГУТ, 2016. - 86 с. : ил. - 540.86 р.

8.2. Дополнительная литература:

1. Косиненко, Н. С. Информационные системы и технологии в экономике [Электронный ресурс] : учебное пособие / Косиненко Н. С. - Москва : Дашков и К, Ай Пи Эр Медиа, 2017. - 304 с. - ISBN 978-5-394-01730-8 : Б. ц. Книга находится в Премиум-версии ЭБС IPRbooks.
2. Богомолова, М. А. Архитектура предприятия [Электронный ресурс] : учебное

пособие / Богомолова М. А. - Самара : Поволжский государственный университет телекоммуникаций и информатики, 2016. - 155 с. - Б. ц. Книга находится в Премиум-версии ЭБС IPRbooks.
3. Умнова, Е. Г. Моделирование бизнес-процессов с применением нотации BPMN [Электронный ресурс] : учебно-методическое пособие / Умнова Е. Г. - Саратов : Вузовское образование, 2017. - 48 с. - ISBN 978-5-4487-0063-7 : Б. ц. Книга находится в Премиум-версии ЭБС IPRbooks.

9. Материально-техническое обеспечение практики

Таблица 8

№ 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 IPRbooks (http://www.iprbookshop.ru)
- ЭБС Лань (https://e.lanbook.com/)
- ЭБС СПбГУТ (http://lib.spbgut.ru)

10.2. Ресурсы информационно-телекоммуникационной сети «Интернет»

- www.sut.ru
- lib.spbgut.ru/jirbis2_spbgut

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.