

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)



Первый проректор проректор по учебной работе
Г.М. Машков
02 04 2020 г.

Регистрационный №_20.05/610-Д

ПРОГРАММА ПРАКТИКИ

Преддипломная практика

(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 «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 основы написания компьютерных приложений - Изучить документацию к средствам защиты, используемым 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.01.03(Пд) 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».

«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 - 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 «Преддипломная практика» 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.;
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;
уметь	использовать стандартные методы проектирования документооборота в организации;
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;
уметь	использовать в разрабатываемых программах механизмы наследования, полиморфизма, обработки исключений;
владеть	методами разработки средств обеспечения информационной безопасности;

Навыки компетенции ПК-3

знать	международные стандарты обеспечения информационной безопасности объектов;
уметь	проводить мониторинг защищенности компьютерных сетей и систем;
владеть	методами защиты на основе российских и международных стандартов;

Навыки компетенции ПК-4

знать	Алгоритмы создания программ;
уметь	готовить необходимую инфраструктуру для проведения теста на проникновение;
владеть	методами проведения аудита безопасности сетей;

Навыки компетенции ПК-5

знать	возможности обеспечения защиты оборудования от ЭМИ, КЗ, скачков напряжения;
уметь	обеспечить защиту оборудования от ЭМИ, КЗ, скачков напряжения;
владеть	методами, обеспечивающими защиту оборудования от ЭМИ, КЗ, скачков напряжения;

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;
уметь	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;

Навыки компетенции ПК-7

знать	классификацию основных типов уязвимостей в системах;
уметь	проводить расследование инцидентов ИБ в различных файловых системах;
владеть	методами моделирования систем информационной безопасности;

Навыки компетенции ПК-8

знать	обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи;
уметь	совершить сборку, ремонт, настройку ПК, ноутбуков и мобильных устройств. Установить и настроить ОС и прикладное ПО;
владеть	базовыми знаниями по настройке сетей, установке и настройке компьютерной техники, сборка компьютерной техники, восстановление данных, знания операционных систем UNIX подобных и Windows подобных.;

Навыки компетенции ПК-9

знать	как проводить проверку информационной безопасности больших данных;
уметь	проводить аудит информационной безопасности информационных систем с большим объемом данных;
владеть	методами проведения аудита безопасности систем;

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	правовые аспекты взаимодействия субъектов на рынке информации;
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	методами управления коллективом исполнителей и принимать управленческие решения;

Навыки компетенции ПК-13

знать	методы управления информационной безопасностью;
уметь	организовать управление информационной безопасностью;
владеть	способностью организовать управление информационной безопасностью;

Навыки компетенции ПК-14

знать	обязанности организатора распространения информации в сети "Интернет";
уметь	настраивать протоколы PPP;
владеть	навыками мониторинга компьютерной сети;

Навыки компетенции ПК-15

знать	виды информации в зависимости от категории доступа и в зависимости от порядка ее предоставления или распространения;
уметь	вводить в эксплуатацию системы и средства обеспечения информационной безопасности;
владеть	навыками работы в команде;

Навыки компетенции ПК-16

знать	организационно-распорядительную, техническую и эксплуатационную документацию;
уметь	настраивать трансляцию сетевых адресов;
владеть	навыками настройки туннелей;

Дополнительные компетенции

Таблица 3

№ п/п	Код компетенции	Наименование компетенции
1	ПС-1	Проведение контрольных проверок работоспособности программно-аппаратных средств защиты информации
2	ПС-3	Формирование политик информационной безопасности
3	ПС-6	Разработка требований по защите информации беспроводных и мобильных компьютерных сетей
4	ПС-8	Проведение анализа безопасности компьютерных систем
5	ПС-9	Проведение сертификации программно-аппаратных средств защиты информации

Планируемые результаты обучения

Таблица 4

Навыки компетенции ПС-1

знать	методы контрольных проверок работоспособности программно-аппаратных средств защиты информации;
уметь	совершить базовую настройку локальной сети и беспроводной локальной сети.;
владеть	методами контрольных проверок работоспособности программно-аппаратных средств защиты информации;

Навыки компетенции ПС-3

знать	актуальную и полную информацию о формировании политик информационной безопасности;
уметь	установить и настроить, оказать помощь в эксплуатации периферийных устройств, оргтехники и техники специального назначения;
владеть	навыками и методами формирования политик информационной безопасности;

Навыки компетенции ПС-6

знать	актуальную и полную информацию по разработке требований по защите информации беспроводных и мобильных компьютерных сетей;
уметь	создавать резервные копии данных, восстановление утраченных;
владеть	навыками по разработке требований по защите информации беспроводных и мобильных компьютерных сетей;

Навыки компетенции ПС-8

знать	актуальную и полную информацию по проведению анализа безопасности компьютерных систем;
уметь	провести анализ безопасности компьютерных систем;
владеть	методами и навыками обеспечения анализа безопасности компьютерных систем;

Навыки компетенции ПС-9

знать	программно-аппаратные средства защиты информации;
--------------	---

уметь	проводить сертификации;
владеть	владеть знаниями в сфере защиты информации;

5. Объем практики и виды учебной работы

Очная форма обучения

Таблица 5

Вид учебной работы		Всего часов	Семестры
			4
Общая трудоемкость	15 ЗЕТ	540	540
Контактная работа с обучающимися			-
Работа под руководством преподавателя		390	390
Анализ данных, подготовка отчета, зачет		150	150.00
Самостоятельная работа обучающихся (СРС)			-
Вид промежуточной аттестации			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	4		
2	Раздел 2. Составление индивидуального плана работы студента	определение и согласование индивидуального плана работы	4		
3	Раздел 3. Выполнение индивидуального задания	получение и выполнение индивидуального задания	4		
4	Раздел 4. Подготовка отчета	оформление и подготовка работы	4		
5	Раздел 5. Защита отчета	выступление и защита работы	4		

6.2. Междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами.

«Преддипломная практика» является базой для написания магистерской диссертации

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. Андрианов, В. И. Инновационное управление рисками информационной безопасности [Электронный ресурс] : учеб. пособие / В. И. Андрианов, А. В. Красов, В. А. Липатников ; рец.: С. Е. Душин, Е. В. Стельмашонок ; Федер. агентство связи, Федер. гос. образовательное бюджет. учреждение высш. проф. образования "С.-Петерб. гос. ун-т телекоммуникаций им. проф. М. А. Бонч-Бруевича". - СПб. : СПбГУТ, 2012. - 396 с. : ил. - Библиогр.: с. 394-395. - ISBN 978-5-91891-092-4 (в обл.) : 320.00 р.
2. Защита информации с помощью маршрутизаторов и коммутаторов [Электронный ресурс] : учебное пособие / Д. И. Кириллов, А. В. Красов, Е. А. Силин, И. А. Ушаков ; рец. В. В. Княжицкий ; Федеральное агентство связи, Федеральное государственное образовательное бюджетное учреждение высшего профессионального образования "Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича". - СПб. : СПбГУТ, 2013. - 62 с. : ил. - 91.33 р.

8.2. Дополнительная литература:

1. Запечников, С. В. Основы построения виртуальных частных сетей. Учебное пособие для вузов [Электронный ресурс] / С. В. Запечников, Н. Г. Милославская, А. И. Толстой. - М. : Горячая линия-Телеком, 2011. - 248 с. : ил. - ISBN 978-5-9912-0215-2 : Б. ц.

9. Материально-техническое обеспечение практики

Таблица 7

№ 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»

Ресурсы информационно-телекоммуникационной сети «Интернет» из указанного перечня являются рекомендуемыми дополнительными (вспомогательными) источниками официальной информации, размещенной на легальных основаниях с открытым доступом. За полноту содержания и качество работу сайтов несет ответственность правообладатель.

Таблица 8

Наименование ресурса	Адрес
Поисковая система google.com	google.ru

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.