

**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 №\_20.05/604-Д

**ПРОГРАММА ПРАКТИКИ**

Научно-исследовательская работа

(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 «Научно-исследовательская работа» 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;
- планирование исследования (выбор темы, обоснование необходимости, определение целей и задач, выдвижение гипотез, формирование программы, подбор средств и инструментария);
- проведение исследования (изучение литературы, сбор, обработка и обобщение данных, объяснение полученных результатов и новых фактов, аргументирование, формулировка выводов);
- оформление отчета о результатах исследования (изучение нормативных требований, формирование структуры и содержания, написание, редактирование, формирование списка использованных источников информации, оформление приложений);
- выступление с докладами на студенческих конференциях по результатам исследований.

## **2. Место практики в структуре основной образовательной программы**

«Научно-исследовательская работа» Б2.В.01.01(Н) 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».

«Научно-исследовательская работа» опирается на знания полученные при изучении предшествующих дисциплин, а также на знания и практические навыки, полученные при прохождении практик(и) «Преддипломная практика».

## **3. Вид, тип, способ, форма проведения практики**

Вид практики - производственная

Тип практики - «Научно-исследовательская работа»

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 «Научно-исследовательская работа» 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-4	способностью разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности
4	ПК-5	способностью анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества
5	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
6	ПК-7	способностью проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента
7	ПК-8	способностью обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи
8	ПК-12	способностью организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения
9	ПК-13	способностью организовать управление информационной безопасностью
10	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
11	ПК-15	способностью организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности
12	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

<b>знать</b>	современные методы научных исследований и информационно-коммуникационных технологий в области организации информационной безопасности социально-экономических информационных систем;
--------------	--

<b>уметь</b>	современные методы научных исследований и информационно-коммуникационных технологий в области организации информационной безопасности социально-экономических информационных систем;
<b>владеть</b>	современные методы научных исследований и информационно-коммуникационных технологий в области организации информационной безопасности социально-экономических информационных систем;

#### Навыки компетенции ПК-1

<b>знать</b>	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;
<b>уметь</b>	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;
<b>владеть</b>	способностью анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты;

#### Навыки компетенции ПК-4

<b>знать</b>	Алгоритмы создания программ; законодательную основу и ограничения, регулирующие санкционированное проведение аудита и теста на проникновение; перечень сведений, составляющих государственную тайну в РФ;
<b>уметь</b>	готовить необходимую инфраструктуру для проведения теста на проникновение; Проводить испытания средств и систем обеспечения информационной безопасности; проводить мониторинг защищенности компьютерных сетей и систем;
<b>владеть</b>	методами проведения аудита безопасности сетей; 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

<b>знать</b>	технологии организации обеспечения информационной безопасности;
<b>уметь</b>	выбирать способы решения прикладных проблем информационной безопасности в условиях становления современного информационного общества;
<b>владеть</b>	основными терминами и понятиями в области информационной безопасности;

#### Навыки компетенции ПК-6

<b>знать</b>	Особый порядок допуска к государственной тайне.;
<b>уметь</b>	проводить мониторинг защищенности компьютерных сетей и систем;
<b>владеть</b>	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

<b>знать</b>	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;
<b>уметь</b>	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;
<b>владеть</b>	методами моделирования систем информационной безопасности; навыками написания отчетов по форензике; навыками обнаружения уязвимостей в корпоративных сетях;

#### Навыки компетенции ПК-8

<b>знать</b>	Основания для отказа должностному лицу или гражданину в допуске к государственной тайне;
<b>уметь</b>	проводить мониторинг защищенности компьютерных сетей и систем;
<b>владеть</b>	способностью обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи;

#### Навыки компетенции ПК-12

<b>знать</b>	принципы работы с большими данными, основные понятия, касающиеся технологий обеспечения информационной безопасности больших данных;
<b>уметь</b>	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;
<b>владеть</b>	способностью организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения;

#### Навыки компетенции ПК-13

<b>знать</b>	организацию управления ИБ;
<b>уметь</b>	производить организацию по управлению ИБ;
<b>владеть</b>	способностью организовать управление информационной безопасностью;

#### Навыки компетенции ПК-14

<b>знать</b>	обязанности организатора распространения информации в сети "Интернет"; принципы работы с большими данными, основные понятия, касающиеся технологий обеспечения информационной безопасности больших данных; принципы работы с большими данными, основные понятия, касающиеся технологий обеспечения информационной безопасности больших данных;
<b>уметь</b>	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;

<b>владеть</b>	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

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

#### Навыки компетенции ПК-16

<b>знать</b>	разработку проектов, бизнес-планов, технической и эксплуатационной документации на системы, средства обеспечения ИБ; специфику технологий обеспечения информационной безопасности объектов защиты;
<b>уметь</b>	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;
<b>владеть</b>	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-6	Разработка требований по защите информации беспроводных и мобильных компьютерных сетей
6	ПС-8	Проведение анализа безопасности компьютерных систем

#### Планируемые результаты обучения

Таблица 4

#### Навыки компетенции ПС-1

<b>знать</b>	современные методы обеспечения целостности и защиты информации;
<b>уметь</b>	выбирать соответствующие организационные и программно-аппаратные средства для организации систем информационной защиты;
<b>владеть</b>	защищать папки и файлы в ОС Windows;

#### Навыки компетенции ПС-2

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

### Навыки компетенции ПС-3

<b>знать</b>	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;
<b>уметь</b>	разрабатывать компоненты политик ИБ с учётом результатов моделирования СЗИ объекта защиты; разрабатывать нормы и политики ИБ; разрабатывать технические решения по защите от несанкционированного доступа межсетевому взаимодействию 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;
<b>владеть</b>	методологией построения политики информационной безопасности инфокоммуникационных систем; навыками и методами формирования политик информационной безопасности; умением формировать и создавать политики ИБ;

### Навыки компетенции ПС-4

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

### Навыки компетенции ПС-6

<b>знать</b>	основную структуру кода защищённого приложения;
<b>уметь</b>	создавать исполняемые файлы из исходного кода;
<b>владеть</b>	навыками по разработке требований по защите информации беспроводных и мобильных компьютерных сетей;



## Навыки компетенции ПС-8

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

## 5. Объем практики и виды учебной работы

Очная форма обучения

Таблица 5

Вид учебной работы		Всего часов	Семестры		
			1	2	3
Общая трудоемкость	21 ЗЕТ	756	324	108	324
<b>Контактная работа с обучающимися</b>			-	-	-
Работа под руководством преподавателя		546	234	78	234
Анализ данных, подготовка отчета, зачет		210	90.00	30.00	90.00
<b>Самостоятельная работа обучающихся (СРС)</b>			-	-	-
Вид промежуточной аттестации			Зачет	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 темы, из списка представленного научным руководителем и последующее согласование	1		
2	Раздел 2. Составление индивидуального плана работы студента	согласование индивидуального плана работ с научным руководителем	1		
3	Раздел 3. Выполнение индивидуального задания	Выполнение индивидуального задания	2		
4	Раздел 4. Подготовка отчета	Предоставление предварительного отчета научному руководителю для согласования	3		
5	Раздел 5. Защита отчета	Проведение зачета по практике с последующим ответом на вопросы согласно с выбранной теме	3		

6.2. Междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами.

«Научно-исследовательская работа» 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. Никитина, Александра Викторовна.**

Сети радиодоступа четвертого поколения. Стандарт LTE : технологии и процедуры : учебное пособие / А. В. Никитина, А. Е. Рыжков ; рец.: И. А. Цикин, Ю. С. Шинаков ; Федеральное агентство связи, Федеральное государственное образовательное бюджетное учреждение высшего профессионального образования "Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича". - СПб. : СПбГУТ, 2012. - 87 с. :

- ил., табл. - 112.86 р. - Текст : непосредственный. Есть автограф: Экз. у3954 ЧЗ : Никитина, Александра Викторовна; Рыжков, Александр Евгеньевич
2. Фокин, Григорий Алексеевич. Планирование систем мобильной связи : учебное пособие : в 2 ч. / Г. А. Фокин, В. Ю. Бабков ; рец.: С. Б. Макаров, М. А. Сиверс ; Федеральное агентство связи, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования "Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича". - СПб. : СПбГУТ. Ч. 2 : Сети UMTS. - 2017. - 111 с. : ил. - 642.00 р.

## 8.2. Дополнительная литература:

1. Никитина, Александра Викторовна.  
Цифровая обработка сигналов в сетях доступа : [Электронный ресурс] : учебное пособие / А. В. Никитина, А. Е. Рыжков ; рец.: А. И. Солонина, С. А. Шпак ; 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. - 82 с. : ил., табл. - 126.82 р.
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](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
3. 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

## 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»

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.