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 2020 г.

Регистрационный №_20.05/602-Д

ПРОГРАММА ПРАКТИКИ

Проектно-технологическая 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 «Проектно-технологическая 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;

2. Место практики в структуре основной образовательной программы

«Проектно-технологическая практика» Б2.В.02.01(П) 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».

«Проектно-технологическая практика» опирается на знания полученные при изучении предшествующих дисциплин, а также на знания и практические навыки, полученные при прохождении практик(и) «Практика по получению первичных профессиональных умений и навыков».

3. Вид, тип, способ, форма проведения практики

Вид практики – производственная

Тип практики – «Проектно-технологическая 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 «Проектно-технологическая практика» студент формирует и демонстрирует следующие компетенции:

Компетенции, установленные ФГОС ВО

Таблица 1

№ п/п	Код компетенции	Наименование компетенции
1	ПК-1	способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации

2	ПК-2	способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач
3	ПК-3	способностью администрировать подсистемы информационной безопасности объекта защиты
4	ПК-4	способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты
5	ПК-5	способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации
6	ПК-6	способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации
7	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
8	ПК-8	способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов
9	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
10	ПК-10	способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности
11	ПК-11	способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов
12	ПК-12	способностью принимать участие в проведении экспериментальных исследований системы защиты информации
13	ПК-13	способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации
14	ПК-14	способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности
15	ПК-15	способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

Планируемые результаты обучения

Таблица 2

Навыки компетенции ПК-1

знать	архитектуру локальных вычислительных сетей, сетевые протоколы стека TCP/IP;
уметь	настраивать виртуальные локальные сети. Маршрутизацию между виртуальными локальными сетями;
владеть	навыками мониторинга компьютерной сети;

Навыки компетенции ПК-2

знать	алгоритмы применения аппаратно-программных средств;
уметь	выполнять Машинно-независимая оптимизации, Распараллеливание, Обфускации, модификации ПО (ПК-2);
владеть	владеть навыками работы с программами и данными;

Навыки компетенции ПК-3

знать	Основные методы администрирования ОС GNULinux.;
уметь	Настраивать политики информационной безопасности операционных систем;
владеть	алгоритмами обработки сетевого трафика стандартами утилитами ОС;

Навыки компетенции ПК-4

знать	Нормативно-правовую документацию по защите информации;
уметь	внедрять протокол IPv6;
владеть	основами методов защиты информации в компьютерных сетях;

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 защиты объектов инфокоммуникаций;
владеть	принципами и навыками инструментальных измерений, используемых в области инженерной защиты объектов инфокоммуникаций;

Навыки компетенции ПК-7

знать	архитектуру построения дата-центров (ПК-7);
уметь	конфигурировать устройства, обеспечивающие работу ЦОД (ПК-7);
владеть	навыками настройки политик безопасности в ЦОД (ПК-7);

Навыки компетенции ПК-8

знать	основные понятия, связанные с лицензированием программного обеспечения;
уметь	пользоваться технической документации при лицензировании ПО;
владеть	основными критериями использования нормативных правовых актов при лицензировании ПО;

Навыки компетенции ПК-9

знать	Нормативно-правовую базу РФ в сфере обеспечения информационной безопасности;
уметь	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;
уметь	анализировать конкретные социально-экономические и социально-правовые ситуации в условиях рыночной экономики, быстро меняющейся технико-экономической конъюктуры и конкурентной среды отрасли (ПК-10);;
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;
уметь	прооводить экспериментальные исследования;
владеть	способностью принимать участие в проведении экспериментальных исследований системы защиты информации;

Навыки компетенции ПК-13

знать	Какие комплексы мер по обеспечению информационной безопасности требуются;
уметь	Поддерживать, организовывать, управлять процессом реализации выполнения комплекса мер;
владеть	Способностью принимать участие в формировании, организации и поддержки выполнения комплекса мер по обеспечению информационной безопасности;

Навыки компетенции ПК-14

знать	понятие, сущность, цели и задачи комплексной системы защиты информации;
уметь	классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;
владеть	методиками проверки защищенности объектов информатизации на соответствие требованиям;

Навыки компетенции ПК-15

знать	Знание нормативно-правовых актов РФ в отношении защиты информации;
уметь	осуществлять приемку и освоение вводимого оборудования в соответствии с действующими нормативами;
владеть	Методами применения нормативно-правовых актов РФ в отношении защиты информации;

Дополнительные компетенции

Таблица 3

№ п/п	Код компетенции	Наименование компетенции
1	ПС-1	способностью формулировать и настраивать политики безопасности операционных систем
2	ПС-2	способностью оценивать угрозы безопасности информации операционных систем
3	ПС-3	способностью противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации операционных систем

4	ПС-4	способностью выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах
5	ПС-5	способностью устанавливать и настраивать антивирусные средства защиты информации в операционных системах
6	ПС-6	способностью проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах
7	ПС-7	способностью оценивать угрозы безопасности информации в компьютерных сетях
8	ПС-8	способностью настраивать правила фильтрации пакетов в компьютерных сетях
9	ПС-9	способностью обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных сетях
10	ПС-10	способностью конфигурировать и контролировать корректность настройки программно-аппаратных средств защиты информации в компьютерных сетях
11	ПС-11	способностью выбирать режимы работы программно-аппаратных средств защиты информации в компьютерных сетях
12	ПС-12	способностью проводить мониторинг функционирования программно-аппаратных средств защиты информации в компьютерных сетях
13	ПС-13	способностью анализировать угрозы безопасности информации программного обеспечения
14	ПС-14	способностью формулировать и обосновывать правила безопасной эксплуатации программного обеспечения
15	ПС-15	способностью анализировать функционирование программного обеспечения с целью определения возможного вредоносного воздействия
16	ПС-16	способностью осуществлять мероприятия по противодействию угрозам безопасности информации, возникающим при эксплуатации программного обеспечения
17	ПС-17	способностью определять порядок функционирования программного обеспечения с целью обеспечения защиты информации
18	ПС-18	способностью анализировать эффективность сформулированных требований к встроенным средствам защиты информации программного обеспечения

Планируемые результаты обучения

Таблица 4

Навыки компетенции ПС-1

знать	Требования ФСТЭК предъявляемые к операционным системам специального назначения.;
уметь	Настраивать политики информационной безопасности операционных систем специального назначения.;
владеть	Основными методами формирования политик безопасности.;

Навыки компетенции ПС-2

знать	методы оценки угрозы безопасности информации операционных систем;
уметь	оценивать угрозы безопасности информации операционных систем;
владеть	методами оценки угрозы безопасности информации операционных систем;

Навыки компетенции ПС-3

знать	Стандартные средства операционных систем по обеспечению информационной безопасности.;

уметь	Анализировать поведение системы, встроенными средствами операционной системы.;
владеть	Методами противодействия вторжению в систему.;

Навыки компетенции ПС-4

знать	режимы работы программно-аппаратных средств защиты информации в операционных системах;
уметь	выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах;
владеть	алгоритмами обработки сетевого трафика стандартами утилитами ОС;

Навыки компетенции ПС-5

знать	основные типы вирусов;
уметь	уметь настраивать антивирусные средства защиты информации в операционных системах;
владеть	навыками работы с антивирусным программным обеспечением;

Навыки компетенции ПС-6

знать	основные средства и методы анализа программных реализаций на предмет уязвимостей. (ПК-2);;
уметь	оценивать опасность обнаруженных уязвимостей программных реализаций (ПС-15);;
владеть	навыками устранения выявленных уязвимостей в программных реализациях (ПК-2);;

Навыки компетенции ПС-7

знать	технологию MPLS;
уметь	настраивать механизмы QoS в сети предприятия;
владеть	основами настройки протокола BGP;

Навыки компетенции ПС-8

знать	знать компьютерные сети;
уметь	работать с правилами фильтрации;
владеть	способностью настраивать правила фильтрации пакетов;

Навыки компетенции ПС-9

знать	принципы построения иерархического дизайна (ПК-1);
уметь	принципы построения иерархического дизайна (ПК-1);
владеть	навыками настройки EtherChannel (ПК-1).;

Навыки компетенции ПС-10

знать	компоненты решений унифицированных взаимодействий Cisco;
уметь	-описывать дополнительные сервисы, которые поддерживаются в решениях Unified Communications Manager и Unified Communications Manager Express (ПС-10);; описывать дополнительные сервисы, которые поддерживаются в решениях Unified Communications Manager и Unified Communications Manager Express;
владеть	- навыками настройки пользователей и базовые сервисы (ПС-10);;

Навыки компетенции ПС-11

знать	режимы работы программно-аппаратных средств защиты информации в компьютерных сетях;

уметь	выбирать режимы работы программно-аппаратных средств защиты информации в компьютерных сетях;
владеть	способностью выбирать режимы работы программно-аппаратных средств защиты информации в компьютерных сетях;

Навыки компетенции ПС-12

знать	архитектуру глобальных сетей и виды виртуальных частных туннелей;
уметь	настраивать протоколы Frame Relay, PPP;
владеть	навыками настройки трансляции сетевых адресов;

Навыки компетенции ПС-13

знать	принципы построения криптосистем с открытым ключом Эль-Гамаля, РША, Рабина, Мас-Элиса (ПС-13);-модель цифровой подписи сообщения. Виды ЭЦП. Основные схемы ЭЦП, включая ЭЦП на основе эллиптических кривых (ПС-13);;
уметь	анализировать угрозы безопасности информации программного обеспечения;
владеть	навыками работы по обеспечению информационной информации программного обеспечения;

Навыки компетенции ПС-14

знать	правила безопасной эксплуатации программного обеспечения;
уметь	формулировать и обосновывать свою позицию;
владеть	основными навыками эксплуатации программного обеспечения;

Навыки компетенции ПС-15

знать	основные средства и методы анализа программных реализаций на предмет уязвимостей. (ПК-2);;
уметь	выявлять уязвимости программных реализаций (ПС-15);;
владеть	вопросами навыками работы с современными дизассемблерами и отладчиками (ПС-15);;

Навыки компетенции ПС-16

знать	меры обеспечения информационной безопасности при эксплуатации программного обеспечения;
уметь	осуществлять мероприятия по противодействию угрозам безопасности информации, возникающим при эксплуатации программного обеспечения;
владеть	навыками работы по обеспечению информационной безопасности;

Навыки компетенции ПС-17

знать	Неэквивалентные преобразования;;
уметь	анализировать дизассемблированный код;
владеть	навыками работы с дизассемблером;

Навыки компетенции ПС-18

знать	методы анализа эффективности сформулированных требований;
уметь	формулировать требования к встроенным средствам защиты информации программного обеспечения;
владеть	навыками анализа эффективности сформулированных требований к встроенным средствам защиты информации программного обеспечения;

5. Объем практики и виды учебной работы

Очная форма обучения

Таблица 5

Вид учебной работы		Всего часов	Семестры	
			4	6
Общая трудоемкость	9 ЗЕТ	324	108	216
Контактная работа с обучающимися			-	-
Работа под руководством преподавателя		234	78	156
Анализ данных, подготовка отчета, зачет		90	30.00	60.00
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	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	6		
4	Раздел 4. Подготовка отчета	Оформление и подготовка работы	6		
5	Раздел 5. Защита отчета	Выступление и защита работы	6		

6.2. Междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами.

Таблица 7

№ п/п	Наименование обеспечиваемых (последующих) дисциплин
1	Преддипломная практика

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. Красов, Андрей Владимирович. Разработка защищенных приложений [Электронный ресурс] : учебное пособие / А. В. Красов, А. Ю. Цветков ; рец. С. Е. Душин ; 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. - 119.87 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.
3. Орлов, С. А. Технологии разработки программного обеспечения. Учебник для вузов. 4-е издание. Стандарт третьего поколения [Электронный ресурс] / С. А. Орлов, Б. Я. Цилькер. - СПб. : Питер, 2012. - 608 с. : ил. - ISBN 978-5-459-01101-2 : Б. ц.

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 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 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.