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
«21» 07 2019 г.

Регистрационный №_19.05/2178-Д

ПРОГРАММА ПРАКТИКИ

Преддипломная практика
(наименование практики)

образовательная программа высшего образования

10.05.02 Информационная безопасность телекоммуникационных систем
(код и наименование направления подготовки / специальности)

Специалист по защите информации
(квалификация)

Безопасность телекоммуникационных систем информационного взаимодействия
(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 «10.05.02 Информационная безопасность телекоммуникационных систем», утвержденным приказом Министерства образования и науки Российской Федерации от 16.11.2016 № 1426, 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).

2. Место практики в структуре основной образовательной программы

«Преддипломная практика» Б2.Б.02.03(Пд) входит в блок 2 учебного плана, который относится к вариативной части, и является обязательной составной частью образовательной программы по направлению «10.05.02 Информационная безопасность телекоммуникационных систем».

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

3. Вид, тип, способ, форма проведения практики

Вид практики – производственная

Тип практики – «Преддипломная практика»

Способ проведения – стационарная; выездная

Форма проведения – дискретно по видам и по периодам проведения практик

Стационарная практика может проводиться в структурных подразделениях университета.

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

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

Компетенции, установленные ФГОС ВО

Таблица 1

№ п/п	Код компетенции	Наименование компетенции
1	ОК-8	способностью к самоорганизации и самообразованию

2	ОПК-1	способностью анализировать физические явления и процессы для формализации и решения задач, возникающих в ходе профессиональной деятельности
3	ОПК-2	способностью применять соответствующий математический аппарат для решения профессиональных задач
4	ОПК-3	способностью применять положения теорий электрических цепей, радиотехнических сигналов, распространения радиоволн, цифровой обработки сигналов, информации и кодирования, электрической связи для решения профессиональных задач
5	ОПК-4	способностью понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации
6	ОПК-5	способностью применять программные средства системного и прикладного назначения, языки, методы и инструментальные средства программирования для решения профессиональных задач
7	ОПК-6	способностью применять методы научных исследований в профессиональной деятельности
8	ОПК-7	способностью применять нормативные правовые акты в своей профессиональной деятельности
9	ОПК-8	способностью применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности
10	ПК-1	способностью осуществлять анализ научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности телекоммуникационных систем
11	ПК-2	способностью формулировать задачи, планировать и проводить исследования, в том числе эксперименты и математическое моделирование, объектов, явлений и процессов телекоммуникационных систем, включая обработку и оценку достоверности их результатов
12	ПК-3	способностью оценивать технические возможности и вырабатывать рекомендации по построению телекоммуникационных систем и сетей, их элементов и устройств
13	ПК-4	способностью участвовать в разработке компонентов телекоммуникационных систем
14	ПК-5	способностью проектировать защищенные телекоммуникационные системы и их элементы, проводить анализ проектных решений по обеспечению заданного уровня безопасности и требуемого качества обслуживания, разрабатывать необходимую техническую документацию с учетом действующих нормативных и методических документов
15	ПК-6	способностью применять технологии обеспечения информационной безопасности телекоммуникационных систем и нормы их интеграции в государственную и международную информационную среду
16	ПК-7	способностью осуществлять рациональный выбор средств обеспечения информационной безопасности телекоммуникационных систем с учетом предъявляемых к ним требований качества обслуживания и качества функционирования
17	ПК-8	способностью проводить анализ эффективности технических и программно-аппаратных средств защиты телекоммуникационных систем
18	ПК-9	способностью участвовать в проведении аттестации телекоммуникационных систем по требованиям защиты информации

19	ПК-10	способностью оценивать выполнение требований нормативных правовых актов и нормативных методических документов в области информационной безопасности при проверке защищенных телекоммуникационных систем, выполнять подготовку соответствующих заключений
20	ПК-11	способностью организовывать работу малых коллективов исполнителей, принимать управленческие решения в сфере профессиональной деятельности, разрабатывать предложения по совершенствованию системы управления информационной безопасностью телекоммуникационной системы
21	ПК-12	способностью выполнять технико-экономические обоснования, оценивать затраты и результаты деятельности организации в области обеспечения информационной безопасности
22	ПК-13	способностью организовывать выполнение требований режима защиты информации ограниченного доступа, разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности телекоммуникационных систем
23	ПК-14	способностью выполнять установку, настройку, обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем
24	ПК-15	способностью проводить инструментальный мониторинг защищенности телекоммуникационных систем, обеспечения требуемого качества обслуживания

Планируемые результаты обучения

Таблица 2

Навыки компетенции ОК-8

знать	основы самоорганизации и самообразованию;
уметь	применять методы самоорганизации и самообразованию;
владеть	способностью к самоорганизации и самообразованию;

Навыки компетенции ОПК-1

знать	теории и методы научного исследования для выявления естественнонаучной сущности проблем в физике и технике; фундаментальные физические законы в области оптики и квантовой физики;
уметь	использовать физические законы при анализе и решении проблем профессиональной деятельности; применять физические законы и математический аппарат для формализации, анализа и выработки путей решения профессиональных задач; решать типовые задачи по основным разделам курса физики, используя методы математического анализа, справочники, каталоги и другие источники информации с применением современных информационных технологий;
владеть	методами решения физических задач, необходимых для профессиональной деятельности; методами экспериментального исследования и обработки полученных результатов с помощью вычислительной техники;

Навыки компетенции ОПК-2

знать	Нормативно-правовую документацию по защите информации; принципы построения криптосистем с открытым ключом; Способы организации и поддержки комплекса мер по информационной безопасности, управления процессом их реализации;
уметь	пользоваться методами теории чисел; Программно реализовать алгоритмы безопасности; рассчитывать основные характеристики и параметры криптографических алгоритмов защиты информации;
владеть	Методами организации защиты объекта от внешних угроз и технологиями защиты информации; навыками анализа основных характеристик систем с открытыми ключами; Особенностями настройки антивирусного программного обеспечения; приемами проектирования типовых алгоритмов криптозащиты и криптоанализа сообщений;

Навыки компетенции ОПК-3

знать	возможности применения современных теоретических и экспериментальных методов исследования с целью создания новых перспективных средств электросвязи и информатики; методы анализа электрических цепей, принципы работы элементов современной радиоэлектронной аппаратуры и физические процессы возникающие в них; основные радиоэлектронные элементы и их применение;принципы работы основных радиоэлектронных схем; современные тенденции в использовании сигнально-кодовых конструкций, технологии ортогонального частотного мультиплексирования и пространственного мультиплексирования.;способы и методы цифровой обработки, фильтрации, спектрального анализа, рандомизации при скачкообразной цифровой частотной модуляции, математические основы блочного и сверточного кодирования.;
уметь	использовать базовые элементы радиоэлектронной аппаратуры; анализировать работу аналоговых схем; определять характеристики ЛДС при заданной математической модели- выполнять синтез и анализ КИХ и БИХ фильтров- применять ДПФ для анализа периодических и конечных сигналов; оценивать спектральную эффективность, выигрыш от использования канального кодирования и помехозащищенность современных и перспективных инфокоммуникационных технологий;; применять на практике методы анализа электрических цепей;
владеть	Методикой оценки необходимого частотного ресурса для обеспечения требуемой пропускной способности современных и перспективных технологий спутниковой, оптической и многоканальной связи.;; навыками компьютерного моделирования базовых методов и алгоритмов ЦОС; навыками чтения электронных схем; экспериментальными методами измерения радиоэлектронных схем;

Навыки компетенции ОПК-4

знать	информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; методы и способы получения хранения и переработки информации,структуру локальных и глобальных компьютерных сетей; структуру и принципы функционирования программы на языке С++;

уметь	определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; применять знания в области информатики при решении профессиональных задач; реализовывать линейные, разветвляющиеся и циклические алгоритмы;
владеть	навыками применения специальных и прикладных программных средств и работы в компьютерных сетях; навыками разработки программного обеспеченья средствами языка С++; способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты;

Навыки компетенции ОПК-5

знать	- основные операции и функции языка программирования С++; - основные типы данных, комбинированные типы данных, классы; - основные уязвимости кода программного кода; - структуру и принципы функционирования языка С++; основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности; основные типы данных, комбинированные типы данных, классы; Основные функциональные возможности и классификации вредоносных программ и антивирусного ПО; Стандартные средства операционных систем по обеспечению информационной безопасности; Угрозы в мобильных платформах: IOS, Android; • основные команды языка Ассемблер; • основные системы вычисления в языке Ассемблер; • основные типы данных и сложные структуры данных языка Ассемблер; • структуру и принципы функционирования языка Ассемблер;
уметь	• использовать основные методы программирования на языке Ассемблер для разработки приложений; • работать с регистрами процессора и оперативной памятью;
владеть	- навыками работы с инструментами и отладочными средствами языка С++; - навыками разработки программного обеспеченья средствами языка С++; - требованиями к информационной безопасности при разработке защищенных приложений; вопросами администрирования ОС MS Windows Server; Навыками работы с эксплоитами; Навыками разработки программ для выявления и устранения вредоносного ПО; навыками разработки программного обеспеченья средствами языка С++; умением выполнять комплекс мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты; • навыками разработки программного обеспеченья средствами языка Ассемблер; • основными методами, способами и средствами получения, хранения, переработки информации средствами языка Ассемблер;

Навыки компетенции ОПК-6

знать	-глобальные проблемы современности и необходимость их научного познания; - основные этапы развития науки, ее структуру и классификацию;

уметь	проводить инструментальные измерения;
владеть	знаниями в сфере информационных технологий;

Навыки компетенции ОПК-7

знать	теоретические основы права, основные положения институтов информационного права, отраженных в нормативно-правовых актах; • Состав участников отраслевого рынка, особенности регулирования их взаимодействия в процессе информационного обмена и оказания услуг; • теоретические основы права, основные положения институтов информационного права, отраженных в нормативно-правовых актах; • функции и методы правового регулирования деятельности в отрасли инфокоммуникаций в соответствии с действующей нормативно-правовой базой и закономерностями развития рыночных отношений в инфокоммуникациях (законы РФ, международные и национальные стандарты, рекомендации МСЭ).; • Характер и этапы научно-технического прогресса, перспективы развития инфокоммуникаций и отраслевого рынка, диктующие необходимость нормативно-правового обеспечения деятельности в условиях глобализации мировой экономики;
уметь	анализировать конкретные социально-экономические и социально-правовые ситуации в условиях рыночной экономики, быстро меняющейся технико-экономической конъюктуры и конкурентной среды отрасли; • анализировать конкретные социально-экономические и социально-правовые ситуации в условиях рыночной экономики, быстро меняющейся технико-экономической конъюктуры и конкурентной среды отрасли;
владеть	методами управления и регулирования правовых отношений отрасли инфокоммуникаций в рыночной среде; • методами управления и регулирования правовых отношений отрасли инфокоммуникаций в рыночной среде;

Навыки компетенции ОПК-8

знать	основные природные и техносферные опасности;
уметь	выбирать методы защиты от опасностей;
владеть	методами защиты в чрезвычайных ситуациях, методами оказания первой помощи; умением разрабатывать и применять мероприятия по охране труда и;

Навыки компетенции ПК-1

знать	международные и отечественные стандарты и регламенты в области технического регулирования и управления качеством при проведении исследований, проектировании, организации технологических процессов и эксплуатации инфокоммуникационных систем, сетей и устройств;; Перспективные технологии и стандарты; Способы организации и поддержки комплекса мер по информационной безопасности, управления процессом их реализации;
уметь	Программно реализовать алгоритмы безопасности; формулировать научно обоснованную проблему;;
владеть	Методами организации защиты объекта от внешних угроз и технологиями защиты информации; навыками самостоятельного научного поиска, реализуемыми при написании текста своей магистерской диссертации;;

Навыки компетенции ПК-2

знать	Безусловно стойкие шифры, способы и условия их реализации; Классификацию шифров (блоковые, потоковые, с открытым ключом); Логические и технологические архитектуры построения доверенных сред передачи на основе группы технологий VPN; международные и отечественные стандарты и регламенты в области технического регулирования и управления качеством при проведении исследований, проектировании, организации технологических процессов и эксплуатации инфокоммуникационных систем, сетей и устройств;; Предмет взлома и защиты от несанкционированного доступа к защищаемой информации; Принципы построения ключевых хэш-функций; Этапы жизненного цикла ключа;
уметь	Настраивать конфигурацию Web-сервера и обеспечивать его защиту от внешних атак; обрабатывать эмпирические данные;; оценивать (в первом приближении) стойкость основных криптосистем и их элементов; • Настраивать конфигурацию Web-сервера и обеспечивать его защиту от внешних атак;
владеть	- представлением о системе управления наукой в России и ее регионах; методами и инструментами моделирования при исследовании систем и сетей инфокоммуникаций.; методами компьютерного моделирования алгоритмов шифрования и расшифрования сообщений; Основной информационной базой по дисциплине – рекомендациями IETF, а также технической документацией производителей оборудования;

Навыки компетенции ПК-3

знать	архитектуру, спецификации, методы построения и применения беспроводных сетей стандартов IEEE 802.11b, 802.11a, 802.11g, 802.16; компоненты решений унифицированных взаимодействий Cisco; • виды и основные характеристики инженерно-технических средств защиты объектов инфокоммуникаций; • возможности технических каналов утечки информации объектов инфокоммуникаций и методы их оценки; • демаскирующие признаки объектов защиты объектов инфокоммуникаций; • методы и способы защиты объектов инфокоммуникаций, показатели эффективности защиты и методы их оценки; • основные источники и носители информации объектов инфокоммуникаций; • основные руководящие, методические и нормативные документы по инженерно-технической защите объектов инфокоммуникаций; • принципы добывания информации; • структуру государственной системы защиты информации; • угрозы безопасности инженерно-технической защиты объектов инфокоммуникаций;

уметь	-описывать дополнительные сервисы, которые поддерживаются в решениях Unified Communications Manager и Unified Communications Manager Express;; использовать спецификации стандарта широкополосного доступа IEEE 802.16 WiMAX при развертывании и эксплуатации городских и региональных систем; Уметь настраивать основные механизмы IP телефонии; • организовать доведение услуг по инженерно-технической защите объектов инфокоммуникаций до пользователей инфокоммуникационными сетями; • организовать и осуществить проверку технического состояния и оценить остаток ресурса сооружений, оборудования и средств инженерной защиты объектов инфокоммуникаций, применить современные методы их обслуживания и ремонта; осуществить поиск и устранение неисправностей, повысить надежность и готовность систем защиты, осуществлять резервирование; • организовать рабочие места, их техническое оснащение, размещение сооружений, средств и оборудования инженерной защиты объектов инфокоммуникаций; • применятьсовременные теоретические и экспериментальные методы исследования с целью создания новых перспективных средств инженерно-технической защиты объектов инфокоммуникаций; организовывать и проводить их испытания с целью оценки соответствия требованиям технических регламентов, международных и национальных стандартов и иных нормативных документов; • проводить расчеты по проекту систем инженерной защиты объектов инфокоммуникаций систем в соответствии с техническим заданием с использованием как стандартных методов, приемов и средств автоматизации проектирования, так и самостоятельно создаваемых оригинальных программ; проводить технико-экономическое обоснования проектных расчетов с использованием современных подходов и методов; • собирать и анализировать информацию для формирования исходных данных для проектирования средств и систем защиты объектов инфокоммуникаций; • составить заявку на оборудование, измерительные устройства и запасные части, подготовить техническую документацию на ремонт и восстановление работоспособности оборудования, средств, систем инженерной защиты объектов инфокоммуникаций; • составлять нормативную документацию (инструкции) по эксплуатационно-техническому обслуживанию оборудования систем инженерной защиты объектов инфокоммуникаций;

владеть	навыками решения задачи конфигурирования пользователей и пользовательских устройств в решениях Cisco Unified Communications Manager и Cisco Unified Communications Manager Express; стандартной терминологией и методами проектирования и моделирования широкополосных беспроводных сетей для коммерческих и прикладных систем широкого назначения; • принципами и навыками инструментальных измерений, используемых в области инженерной защиты объектов инфокоммуникаций; • современными теоретическими и экспериментальными методами исследования с целью создания новых перспективных средств инженерной защиты объектов инфокоммуникаций; организовывать и проводить их испытания с целью оценки соответствия требованиям технических регламентов, международных и национальных стандартов и иных нормативных документов; • способностями к разработке проектной и рабочей технической документации, оформлению законченных проектно-конструкторских работ в области инженерно-технической защиты объектов инфокоммуникаций в соответствии с нормами и стандартами; готовности к контролю соответствия разрабатываемых проектов и технической документации стандартам, техническим условиям и другим нормативным документам; • способностями осуществить монтаж, наладку, настройку, испытания и сдачу в эксплуатацию сооружений, средств и оборудования систем инженерной защиты объектов инфокоммуникаций; • способностями осуществить приемку, освоение и эксплуатацию вводимого оборудования инженерно-технической защиты объектов инфокоммуникаций в соответствии с действующими нормативами;

Навыки компетенции ПК-4

знать	основные нормативные правовые документы, международные и отечественные стандарты в области информационных систем (ИС) и технологий;;
уметь	пользоваться основными нормативными документами РФ;
владеть	навыками поиска необходимых нормативных и законодательных документов и навыками работы с ними в области ИС;

Навыки компетенции ПК-5

знать	Основные модели развертывания виртуальных частных сетей (VPN); • виды и основные характеристики инженерно-технических средств защиты объектов инфокоммуникаций; • возможности технических каналов утечки информации объектов инфокоммуникаций и методы их оценки; • демаскирующие признаки объектов защиты объектов инфокоммуникаций; • методы и способы защиты объектов инфокоммуникаций, показатели эффективности защиты и методы их оценки; • основные источники и носители информации объектов инфокоммуникаций; • основные руководящие, методические и нормативные документы по инженерно-технической защите объектов инфокоммуникаций; • принципы добывания информации; • структуру государственной системы защиты информации; • угрозы безопасности инженерно-технической защиты объектов инфокоммуникаций;

уметь	ориентироваться в системе законодательства и нормативных правовых актов, регламентирующих область ИС; • организовать доведение услуг по инженерно-технической защите объектов инфокоммуникаций до пользователей инфокоммуникационными сетями; • организовать и осуществить проверку технического состояния и оценить остаток ресурса сооружений, оборудования и средств инженерной защиты объектов инфокоммуникаций, применить современные методы их обслуживания и ремонта; осуществить поиск и устранение неисправностей, повысить надежность и готовность систем защиты, осуществлять резервирование; • организовать рабочие места, их техническое оснащение, размещение сооружений, средств и оборудования инженерной защиты объектов инфокоммуникаций; • применятьсовременные теоретические и экспериментальные методы исследования с целью создания новых перспективных средств инженерно-технической защиты объектов инфокоммуникаций; организовывать и проводить их испытания с целью оценки соответствия требованиям технических регламентов, международных и национальных стандартов и иных нормативных документов; • проводить расчеты по проекту систем инженерной защиты объектов инфокоммуникаций систем в соответствии с техническим заданием с использованием как стандартных методов, приемов и средств автоматизации проектирования, так и самостоятельно создаваемых оригинальных программ; проводить технико-экономическое обоснования проектных расчетов с использованием современных подходов и методов; • собирать и анализировать информацию для формирования исходных данных для проектирования средств и систем защиты объектов инфокоммуникаций; • составить заявку на оборудование, измерительные устройства и запасные части, подготовить техническую документацию на ремонт и восстановление работоспособности оборудования, средств, систем инженерной защиты объектов инфокоммуникаций; • составлять нормативную документацию (инструкции) по эксплуатационно-техническому обслуживанию оборудования систем инженерной защиты объектов инфокоммуникаций;

владеть	принципами и навыками инструментальных измерений, используемых в области инженерной защиты объектов инфокоммуникаций; Разрабатывать архитектуру доверенной среды передачи в соответствии с общими требованиями и условиями ситуации в виде ТЗ; • принципами и навыками инструментальных измерений, используемых в области инженерной защиты объектов инфокоммуникаций; • современными теоретическими и экспериментальными методами исследования с целью создания новых перспективных средств инженерной защиты объектов инфокоммуникаций; организовывать и проводить их испытания с целью оценки соответствия требованиям технических регламентов, международных и национальных стандартов и иных нормативных документов; • способностями к разработке проектной и рабочей технической документации, оформлению законченных проектно-конструкторских работ в области инженерно-технической защиты объектов инфокоммуникаций в соответствии с нормами и стандартами; готовности к контролю соответствия разрабатываемых проектов и технической документации стандартам, техническим условиям и другим нормативным документам; • способностями осуществить монтаж, наладку, настройку, испытания и сдачу в эксплуатацию сооружений, средств и оборудования систем инженерной защиты объектов инфокоммуникаций; • способностями осуществить приемку, освоение и эксплуатацию вводимого оборудования инженерно-технической защиты объектов инфокоммуникаций в соответствии с действующими нормативами;

Навыки компетенции ПК-6

знать	методы проведения научных исследований и расчетов; методы проведения научных исследований и расчетов;;
уметь	вести библиографическую работу с привлечением современных информационных технологий; вести библиографическую работу с привлечением современных информационных технологий;;
владеть	методами и инструментами моделирования при исследовании систем и сетей инфокоммуникаций; методами и инструментами моделирования при исследовании систем и сетей инфокоммуникаций.;

Навыки компетенции ПК-7

знать	Законодательную основу и ограничения, регулирующие санкционированное проведение аудита и теста на проникновение; понятие, сущность, цели и задачи комплексной системы защиты информации;
уметь	готовить необходимую инфраструктуру для проведения теста на проникновение; классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; Составлять план аудита и тестирования на проникновения в зависимости от требуемого уровня анализа и используемых механизмов;
владеть	методами проведения аудита безопасности сетей; методиками проверки защищенности объектов информатизации на соответствие требованиям безопасности информации; Основными механизмами проведения теста на проникновение и программным обеспечением, используемым для проведения этого теста;

Навыки компетенции ПК-8

знать	- Архитектуру микропроцессоров 8080 и 8085; - Классификацию регистров памяти и методов ввода-вывода; - Структурные схемы программно-аппаратных средств защиты информации на основе микропроцессоров 8086/8088 и сопроцессоров 8087; Как проводить расследование инцидентов безопасности в ОС Windows, Linux, MAC OS; классификацию основных типов уязвимостей в системах; методы проведения научных исследований и расчетов;; Методы расследования инцидентов информационной безопасности реального мира при помощи различных аспектов цифровой форензики, включая операционные системы, компьютерные сети, файловые системы и системы анализа памяти;
уметь	- Применять на практике полученные теоретические знания, для проведения оценок используемых систем защиты информации; - Работать со средой разработки современных программно-аппаратных средств микроконтроллерной техники; Готовить необходимую инфраструктуру для проведения теста на проникновение; организовывать самостоятельную и коллективную научно-исследовательскую работу;; проводить аудит систем безопасности в корпоративных системах; Проводить расследование инцидентов ИБ в компьютерных сетях, включая дампы трафика и анализ функций сетевых приложений; Проводить расследование инцидентов ИБ в различных файловых системах, включая FAT, NTFS, Ext и HFS; Составлять план аудита и тестирования на проникновения в зависимости от требуемого уровня анализа и используемых механизмов;
владеть	- Основами методов построения программно-аппаратных средств защиты информации на основе микроконтроллерной техники; - Основами программирования на языках C/C++ для создания приложений для обработки информации на микроконтроллерах; - Основами программирования на языке Ассемблер для создания приложений для обработки информации на микроконтроллерах; навыками обнаружения уязвимостей в корпоративных сетях; навыками самостоятельного научного поиска, реализуемыми при написании текста своей магистерской диссертации;; Основными механизмами проведения теста на проникновение и программным обеспечением, используемым для проведения этого теста;

Навыки компетенции ПК-9

знать	Законодательную основу и ограничения, регулирующие санкционированное проведение аудита и теста на проникновение;
уметь	Составлять план аудита и тестирования на проникновения в зависимости от требуемого уровня анализа и используемых механизмов;
владеть	Основными механизмами проведения теста на проникновение и программным обеспечением, используемым для проведения этого теста;

Навыки компетенции ПК-10

знать	Состав участников отраслевого рынка, особенности регулирования их взаимодействия в процессе информационного обмена и оказания услуг; структуру государственной системы защиты информации; • Состав участников отраслевого рынка, особенности регулирования их взаимодействия в процессе информационного обмена и оказания услуг; • теоретические основы права, основные положения институтов информационного права, отраженных в нормативно-правовых актах; • функции и методы правового регулирования деятельности в отрасли инфокоммуникаций в соответствии с действующей нормативно-правовой базой и закономерностями развития рыночных отношений в инфокоммуникациях (законы РФ, международные и национальные стандарты, рекомендации МСЭ).; • Характер и этапы научно-технического прогресса, перспективы развития инфокоммуникаций и отраслевого рынка, диктующие необходимость нормативно-правового обеспечения деятельности в условиях глобализации мировой экономики;
уметь	анализировать конкретные социально-экономические и социально-правовые ситуации в условиях рыночной экономики, быстро меняющейся технико-экономической конъюктуры и конкурентной среды отрасли; применять современные теоретические и экспериментальные методы исследования с целью создания новых перспективных средств инженерно-технической защиты объектов инфокоммуникаций; организовывать и проводить их испытания с целью оценки соответствия требованиям технических регламентов, международных и национальных стандартов и иных нормативных документов; • анализировать конкретные социально-экономические и социально-правовые ситуации в условиях рыночной экономики, быстро меняющейся технико-экономической конъюктуры и конкурентной среды отрасли;
владеть	Знаниями о правовом обеспечении защиты информации; навыками лицензирования программного обеспечения; • методами управления и регулирования правовых отношений отрасли инфокоммуникаций в рыночной среде;

Навыки компетенции ПК-11

знать	методы и средства контроля качества продукции, организацию и технологию стандартизации и сертификации продукции;
уметь	примерять средства измерений для контроля качества продукции и технологических процессов;
владеть	средствами и методами повышения безопасности и экологичности технических средств и технологических процессов;

Навыки компетенции ПК-12

знать	международные и отечественные стандарты и регламенты в области технического регулирования и управления качеством при проведении исследований, проектировании, организации технологических процессов и эксплуатации инфокоммуникационных систем, сетей и устройств;; факторы, влияющие на организацию комплексной системы защиты информации;
уметь	ставить цель и задачи для самостоятельного научного поиска; формировать комплекс мер по защите информации на предприятии и оценивать их эффективность на основе заданных требований по безопасности информации;
владеть	методами и инструментами моделирования при исследовании систем и сетей инфокоммуникаций.;

Навыки компетенции ПК-13

знать	требования режима защиты информации ограниченного доступа;

уметь	разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности телекоммуникационных систем;
владеть	знаниями о режимах защиты информации ограниченного доступа;

Навыки компетенции ПК-14

знать	- компоненты решений унифицированных взаимодействий Cisco; архитектуру локальных вычислительных сетей, сетевые протоколы стека TCP/IP; архитектуру построения дата-центров; виды моделей, описывающих процессы защиты информации; использование IP-адресации в проекте компьютерной сети; методы виртуализации; методы доступа в беспроводных сетях ; - общие методы генерации информационных символов (ПК-14); - технологии расширения спектра; методы кодирования, модуляции, преобразования информации; основные принципы адресации и коммутации в корпоративной сети; основные принципы работы сетей SDN; структурированную модель OSI; этапы разработки требований к веб-приложениям, диаграммы и методы уровня анализа и проектирования веб-приложения, подходы к проектированию веб-интерфейса, архитектурные шаблоны Web-приложений, элементы языка UML применительно для Web-приложений;
уметь	- использовать методы построения и применения беспроводных сетей для создания локальных сетей Wi-Fi; - основные принципы адресации и коммутации в корпоративной сети .- определять структуру сообщений сигнализации и медиапотока;; выполнять анализ прецедентов, осуществлять выбор архитектурного шаблона, составлять описание требований к системе, строить модель прецедентов, диаграммы последовательностей, строить диаграмму пакетов, сотрудничества, видов деятельности, выполнять построение диаграмм путей в сайте, составлять тематическую схему, выполнять интерактивную раскадровку, осуществлять функциональную спецификацию, выполнять инвентарную опись контента, строить схему сайта, составлять словарь схемы сайта, выполнять построение логическ; Использовать совместно с технологиями VPN механизмы аутентификации и авторизации для организации полной цепи доверия в открытых средах передачи; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; конфигурировать устройства, обеспечивающие работу ЦОД; настраивать виртуальные частные сети; настраивать механизмы защиты данных в ЦОД; обнаруживать и устранять неполадки с помощью служебных и диагностических программ; описывать существующую компьютерную сеть, описывать требования (влияние используемых приложений, требования пользователей, технические параметры и др.); Разворачивать инфраструктуры виртуальных частных в соответствии с ТЗ различной степени сложности и вложенности; разрабатывать схему IP-адресации; Реализовывать основные принципы адресации и коммутации в корпоративной сети; устанавливать компьютерную сеть, модернизировать ее компоненты в соответствии с нуждами клиента, выполнять профилактическое обслуживание и устранять неполадки;

владеть	компетенциями IT-менеджера: основного уровня по разработке архитектуры и проектированию веб-приложения; навыками конфигурации базовых команд управления сетевыми устройствами; навыками монтажа кабелей «витая пара» и подключение компьютера к сети; навыками настройки адресации в сети; навыками настройки политик безопасности в ЦОД; навыками настройки пользователей и базовые сервисы; навыками обеспечения защиты, целостности и доступности данных; навыками решения задачи конфигурирования пользователей и пользовательских устройств в решениях Cisco Unified Communications Manager и Cisco Unified Communications Manager Express; стандартной терминологией и методами проектирования и моделирования широкополосных беспроводных сетей для коммерческих и прикладных систем широкого назначения; технологией разработки организационно-функциональной структуры и комплекса нормативно-методического обеспечения комплексной защиты информации на предприятии;

Навыки компетенции ПК-15

знать	Как проводить расследование инцидентов безопасности в ОС Windows, Linux, MAC OS; международные и отечественные стандарты и регламенты в области технического регулирования и управления качеством при проведении исследований, проектировании, организации технологических процессов и эксплуатации инфокоммуникационных систем, сетей и устройств;; основные принципы, методы и методологию проведения тестирования на проникновение в аудируемой организации;
уметь	- выбирать адекватные поставленной научно-исследовательской задаче научные методы; Проводить расследование инцидентов ИБ в компьютерных сетях, включая дампы трафика и анализ функций сетевых приложений; Проводить расследование инцидентов ИБ в различных файловых системах, включая FAT, NTFS, Ext и HFS; составлять план аудита и тестирования на проникновения в зависимости от требуемого уровня анализа и используемых механизмов;
владеть	навыками написания отчетов по форензике; навыками самостоятельного научного поиска, реализуемыми при написании текста своей магистерской диссертации;; основными механизмами проведения теста на проникновение и программным обеспечением, используемым для проведения этого теста;

Дополнительные компетенции

Таблица 3

№ п/п	Код компетенции	Наименование компетенции
1	ПСК-12.1	способностью выполнять декомпозицию сложных информационных систем, формулировать показатели их эффективности с целью построения корректной концептуальной модели систем
2	ПСК-12.2	способностью обоснованно выбирать и (или) строить адекватные, математические и алгоритмические модели, в том числе с помощью высокоуровневых средств, для эффективного проектирования телекоммуникационных систем информационного взаимодействия

3	ПСК-12.3	способностью обоснованно выбирать и применять адекватные методы кодирования для построения высокоэффективных телекоммуникационных систем информационного взаимодействия и систем управления их поведением
4	ПСК-12.4	способностью анализировать информационные потоки на пакетном уровне, оценивать реальный уровень безопасности информационного взаимодействия и предлагать эффективные меры для его повышения
5	ПСК-12.5	способностью применять стандартные средства для анализа программного кода кода с целью оценки уровня его защиты от исследования и поиска несанкционированного или вредоносного вмешательства в работу телекоммуникационных систем информационного взаимодействия

Планируемые результаты обучения

Таблица 4

Навыки компетенции ПСК-12.1

знать	основные понятия, термины, определения в бизнес-процессах, а также понятия анализа видов информации, в которых данные процессы проявляются: учредительная и лицензионная база организации, правовая сфера бизнеса, внутренняя нормативная база организации, внешняя и внутренняя отчетность, материальные и информационные активы;
уметь	использовать методы анализа процессов для определения актуальных угроз организации, методы оценки уровня информационной безопасности организации, методы противодействия «внутренним» угрозам информационной безопасности организации, методы анализа рисков информационной безопасности, методы организационного проектирования, методы управления информационными активами организации;
владеть	навыками использования методов изучения структуры современной коммерческой организации и подходов к управлению службой защиты информации как систематической практической деятельности коллегиальных органов управления организацией и руководителя службы, направленной на формирование и поддержание концептуальных и организационных основ деятельности организации и эффективное выполнение поставленных задач;

Навыки компетенции ПСК-12.2

знать	высокоуровневые средства, для эффективного проектирования;
уметь	выбирать и (или) строить адекватные, математические и алгоритмические модели;
владеть	способностью обоснованно выбирать и (или) строить адекватные, математические и алгоритмические модели;

Навыки компетенции ПСК-12.3

знать	математический аппарат используемый при построении телекоммуникационных систем; принципы построения высокоэффективных телекоммуникационных систем;
уметь	анализировать телекоммуникационные сигналы и системы; управлять поведением телекоммуникационных систем информационного взаимодействия и систем;
владеть	методами математического анализа и расчета сигналов и систем; способностью обоснованно выбирать и применять адекватные методы кодирования;

Навыки компетенции ПСК-12.4

знать	Стек протоколов IPSEC .Методы защиты сетевых устройств и систем;
уметь	разрабатывать комплексную политику сетевой безопасности .конфигурировать систему предотвращения вторжений (IPS);
владеть	навыками настройки статических (site-to-site) VPN соединений .навыками конфигурирования устройств локальной сети для контроля доступа;

Навыки компетенции ПСК-12.5

знать	работу телекоммуникационных систем информационного взаимодействия;
уметь	оценивать уровень защиты кода от исследования и поиска несанкционированного или вредоносного вмешательства;
владеть	способностью применять стандартные средства для анализа программного кода;

5. Объем практики и виды учебной работы

Очная форма обучения

Таблица 5

Вид учебной работы		**Всего часов**	**Семестры**
			11
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	11		
2	Раздел 2. Составление индивидуального плана работы студента	Определение и согласование индивидуального плана работы	11		
3	Раздел 3. Выполнение индивидуального задания	Получение и выполнение индивидуального задания	11		
4	Раздел 4. Подготовка отчета	Оформление и подготовка работы	11		
5	Раздел 5. Защита отчета	Выступление и защита работы	11		

6.2. Междисциплинарные связи с обеспечиваемыми (последующими)

дисциплинами.

«Преддипломная практика» является базой для написания дипломного проекта

7. Методические рекомендации по организации проведения практики и формы отчетности

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

Перед началом прохождения практики студент должен пройти инструктаж о правилах поведения и технике безопасности на рабочем месте, получить индивидуальное задание и ознакомиться с соответствующими должностными инструкциями и регламентными документами.

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

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

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

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

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

8. Учебно-методическое обеспечение практики

8.1. Основная литература:

1. Колесов, Ю.
   Моделирование систем. Объектно-ориентированный подход : [Электронный ресурс] / Ю. Колесов, Ю. Сениченков. - Санкт-Петербург : БХВ-Петербург, 2012. - 192 с. : ил. - URL: http://ibooks.ru/reading.php?productid=24857. - ISBN 978-5-94157-579-3 : Б. ц.
2. Губарев, В. В.
   Квалификационные исследовательские работы : [Электронный ресурс] : учеб.

пособие / В. В. Губарев, О. В. Казанская. - 2-е изд., испр. - Новосибирск : НГТУ, 2014. - 80 с. - URL: https://e.lanbook.com/book/118102. - ISBN 978-5-7782-2472-8 : Б. ц. Книга из коллекции НГТУ - Инженерно-технические науки. Утверждено Редакционно-издательским советом университета в качестве учебного пособия

8.2. Дополнительная литература:

1. Кацнельсон, Лев Нисонович.
   Система цифрового радиовещания DRM : [Электронный ресурс] : учебное пособие / Л. Н. Кацнельсон ; рец.: А. М. Зильберштейн, А. П. Ефимов, О. В. Украинский ; Министерство Российской Федерации по связи и информатизации, СПбГУТ им. проф. М. А. Бонч-Бруевича, Факультет дополнительных видов обучения. - СПб. : СПбГУТ, 2003. - 42 с. : ил. - 29.26 р.
2. Кузнецов, М. А.
   Радиоприемники АМ, ОМ, ЧМ сигналов : пособие по проектированию / М. А. Кузнецов, Р. С. Сенина. - 7-е изд., испр. и перераб. - СПб. : Линk, 2006. - 120 с. : ил. - Библиогр. : с. 108. - 83.05 р. - Текст : непосредственный. Прил. : с. 109-118

3. Модели и архитектуры электронного предприятия : монография / М. Ю. Арзуманян [и др.] ; ред. Ю. В. Арзуманян. - СПб. : Деан, 2009. - 272 с. : ил, табл. - Библиогр. в конце глав. - ISBN 978-5-93630-782-9 : 300.00 р. - Текст : непосредственный.
4. Макаров, В. В.
   Управление качеством : учебное пособие / В. В. Макаров, Т. Н. Старкова, В. И. Гусев ; 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. - 83 с. : ил. - 127.14 р. - Текст : непосредственный.
5. Ковалгин, Ю. А.
   Аудиотехника. Учебник для вузов : [Электронный ресурс] / Ю. А. Ковалгин, Э. И. Вологдин. - М. : Горячая линия-Телеком, 2013. - 742 с. : ил. - URL: http://ibooks.ru/reading.php?productid=333991. - ISBN 978-5-9912-0241-1 : Б. ц.
6. Шелухин, О. И.
   Моделирование информационных систем. Учебное пособие для вузов : [Электронный ресурс] / О. И. Шелухин. - М. : Горячая линия-Телеком, 2012. - 516 с. : ил. - URL: http://ibooks.ru/reading.php?productid=334050. - ISBN 978-5-9912-0193-3 : Б. ц.
7. Сафин, Р. Г.
   Основы научных исследований. Организация и планирование эксперимента : [Электронный ресурс] : учебное пособие / Р. Г. Сафин, А. И. Иванов, Н. Ф. Тимербаев. - Казань : КНИТУ, 2013. - 156 с. - URL: http://e.lanbook.com/books/element.php?pl1_id=73344. - ISBN 978-5-7882-1414-2 : Б. ц. Книга из коллекции КНИТУ - Лесное хозяйство и лесоинженерное дело
8. Згонник, Л. В.
   Организационное поведение : [Электронный ресурс] : учебник / Л. В. Згонник. - М.

: Дашков и К, 2017. - 232 с. - URL: https://e.lanbook.com/book/93393. - ISBN 978-5-394-01733-9 : Б. ц. Книга из коллекции Дашков и К - Экономика и менеджмент. Рекомендовано уполномоченным учреждением Министерства образования и науки РФ — Государственным университетом управления в качестве учебника для студентов высших учебных заведений, обучающихся по направлению подготовки «Менеджмент» . - [Б. м. : б. и.]. - https://e.lanbook.com/book/70550

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.