Приложение А

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)

УТВЕРЖДЕН

на заседании кафедры № 10 от 19.06.2019

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ПРАКТИКЕ

Производственная практика
(Вид практики)

Преддипломная практика
(Наименование (тип) практики)

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)

Санкт-Петербург

1. Общие положения

Фонд оценочных средств (ФОС) по практике используется в целях нормирования процедуры оценивания качества подготовки и осуществляет установление соответствия учебных достижений запланированным результатам обучения и требованиям образовательной программы.

Процедуры оценивания применяются при проведении текущего контроля успеваемости и промежуточной аттестации студентов по практике.

Основным механизмом оценки качества подготовки и формой контроля учебной работы студентов являются текущий контроль успеваемости и промежуточная аттестация. Общие требования к процедурам проведения текущего контроля и промежуточной аттестации определяет внутренний локальный акт университета: Положение о текущем контроле успеваемости и промежуточной аттестации обучающихся.

1.1.Цель и задачи текущего контроля.

Цель текущего контроля – систематическая проверка степени освоения программы производственной практики «Преддипломная практика», знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций и обеспечивающих достижение планируемых результатов освоения образовательной программы.

Задачи текущего контроля:

1. обнаружение и устранение пробелов в процессе прохождения практики;
2. своевременное выполнение корректирующих действий по содержанию и организации процесса обучения;
3. подготовка к промежуточной аттестации.

При прохождении практики реализуется традиционная система поэтапного оценивания уровня освоения. За каждый этап практики студенты получают оценку .

1.2.Цель и задачи промежуточной аттестации студентов по практике.

Цель промежуточной аттестации – проверка достижения планируемых результатов освоения образовательной программы за время прохождения практики и уровня сформированности профессиональных компетенций после ее завершения.

Промежуточная аттестация проходит в форме зачета.

Задачи промежуточной аттестации:

1. определение индивидуального учебного рейтинга студентов;
2. определение уровня сформированности элементов профессиональных компетенций.

2. Перечень компетенций с указанием этапов их закрепления в процессе прохождения практики

2.1.Перечень компетенций.

ОК-8 способностью к самоорганизации и самообразованию

ОПК-1 способностью анализировать физические явления и процессы для формализации и решения задач, возникающих в ходе профессиональной деятельности

ОПК-2 способностью применять соответствующий математический аппарат для решения профессиональных задач

ОПК-3 способностью применять положения теорий электрических цепей, радиотехнических сигналов, распространения радиоволн, цифровой обработки сигналов, информации и кодирования, электрической связи для решения профессиональных задач

ОПК-4 способностью понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации

ОПК-5 способностью применять программные средства системного и прикладного назначения, языки, методы и инструментальные средства программирования для решения профессиональных задач

ОПК-6 способностью применять методы научных исследований в профессиональной деятельности

ОПК-7 способностью применять нормативные правовые акты в своей профессиональной деятельности

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

ПК-1 способностью осуществлять анализ научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности телекоммуникационных систем

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

ПК-3 способностью оценивать технические возможности и вырабатывать рекомендации по построению телекоммуникационных систем и сетей, их элементов и устройств

ПК-4 способностью участвовать в разработке компонентов телекоммуникационных систем

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

ПК-6 способностью применять технологии обеспечения информационной безопасности телекоммуникационных систем и нормы их интеграции в государственную и международную информационную среду

ПК-7 способностью осуществлять рациональный выбор средств обеспечения информационной безопасности телекоммуникационных систем с учетом предъявляемых к ним требований качества обслуживания и качества функционирования

ПК-8 способностью проводить анализ эффективности технических и программно-аппаратных средств защиты телекоммуникационных систем

ПК-9 способностью участвовать в проведении аттестации телекоммуникационных систем по требованиям защиты информации

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

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

ПК-12 способностью выполнять технико-экономические обоснования, оценивать затраты и результаты деятельности организации в области обеспечения информационной безопасности

ПК-13 способностью организовывать выполнение требований режима защиты информации ограниченного доступа, разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности телекоммуникационных систем

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

ПК-15 способностью проводить инструментальный мониторинг защищенности телекоммуникационных систем, обеспечения требуемого качества обслуживания

ПСК-12.1 способностью выполнять декомпозицию сложных информационных систем, формулировать показатели их эффективности с целью построения корректной концептуальной модели систем

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

ПСК-12.3 способностью обоснованно выбирать и применять адекватные методы кодирования для построения высокоэффективных телекоммуникационных систем информационного взаимодействия и систем управления их поведением

ПСК-12.4 способностью анализировать информационные потоки на пакетном уровне, оценивать реальный уровень безопасности информационного взаимодействия и предлагать эффективные меры для его повышения

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

2.2.Этапы формирования компетенций.

Таблица 1

Код компетенции	Этап формирования компетенции	Вид учебной работы	Тип контроля	Форма контроля

ОК-8, ОПК-1, ОПК-2, ОПК-3, ОПК-4, ОПК-5, ОПК-6, ОПК-7, ОПК-8, ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6, ПК-7, ПК-8, ПК-9, ПК-10, ПК-11, ПК-12, ПК-13, ПК-14, ПК-15, ПСК-12.1, ПСК-12.2, ПСК-12.3, ПСК-12.4, ПСК-12.5	информационный	самостоятельная работа	текущий	собеседование, проверка отчета по практике
	практико-ориентированный	консультации, самостоятельная работа	текущий	проверка дневника * по практике
	оценочный	аттестация	промежу-точный	зачет

* в соответствии с Положением о практике обучающихся, осваивающих основные профессиональные программы высшего образования.

3. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

3.1.Описание показателей оценивания компетенций на различных этапах их формирования.

Таблица 2

Этапы обучения	Оценочные средства
ИНФОРМАЦИОННЫЙ ЭТАП:	собеседование, отчет по практике, презентация
ПРАКТИКО-ОРИЕНТИРОВАННЫЙ ЭТАП:	презентация, дневник практики
ОЦЕНОЧНЫЙ ЭТАП:	зачет, дневник практики, отчет по практике, отзыв с места прохождения практики

КОД КОМПЕТЕНЦИИ: ОК-8
ПОКАЗАТЕЛИ, КРИТЕРИИ ОЦЕНИВАНИЯ (планируемые результаты обучения)
ЗНАЕТ:основы самоорганизации и самообразованию;
УМЕЕТ:применять методы самоорганизации и самообразованию;
ВЛАДЕЕТ:способностью к самоорганизации и самообразованию;

КОД КОМПЕТЕНЦИИ: ОПК-1
ПОКАЗАТЕЛИ, КРИТЕРИИ ОЦЕНИВАНИЯ (планируемые результаты обучения)
ЗНАЕТ:теории и методы научного исследования для выявления естественнонаучной сущности проблем в физике и технике;
фундаментальные физические законы в области оптики и квантовой физики;
УМЕЕТ: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;
ВЛАДЕЕТ:методами решения физических задач, необходимых для профессиональной деятельности;
методами экспериментального исследования и обработки полученных результатов с помощью вычислительной техники;

КОД КОМПЕТЕНЦИИ: ОПК-2
ПОКАЗАТЕЛИ, КРИТЕРИИ ОЦЕНИВАНИЯ (планируемые результаты обучения)
ЗНАЕТ: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;
УМЕЕТ:пользоваться методами теории чисел;
Программно реализовать алгоритмы безопасности;
рассчитывать основные характеристики и параметры криптографических алгоритмов защиты информации;
ВЛАДЕЕТ: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;

КОД КОМПЕТЕНЦИИ: ОПК-3
ПОКАЗАТЕЛИ, КРИТЕРИИ ОЦЕНИВАНИЯ (планируемые результаты обучения)
ЗНАЕТ: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.;
УМЕЕТ: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;
ВЛАДЕЕТ: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;

КОД КОМПЕТЕНЦИИ: ОПК-4
ПОКАЗАТЕЛИ, КРИТЕРИИ ОЦЕНИВАНИЯ (планируемые результаты обучения)
ЗНАЕТ: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++;
УМЕЕТ: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;
ВЛАДЕЕТ: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;

КОД КОМПЕТЕНЦИИ: ОПК-5
ПОКАЗАТЕЛИ, КРИТЕРИИ ОЦЕНИВАНИЯ (планируемые результаты обучения)
ЗНАЕТ:- 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;
УМЕЕТ:• использовать основные методы программирования на языке Ассемблер для разработки приложений;
• работать с регистрами процессора и оперативной памятью;
ВЛАДЕЕТ:- 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;

КОД КОМПЕТЕНЦИИ: ОПК-6
ПОКАЗАТЕЛИ, КРИТЕРИИ ОЦЕНИВАНИЯ (планируемые результаты обучения)
ЗНАЕТ:-глобальные проблемы современности и необходимость их научного познания; - основные этапы развития науки, ее структуру и классификацию;
УМЕЕТ:проводить инструментальные измерения;
ВЛАДЕЕТ:знаниями в сфере информационных технологий;

КОД КОМПЕТЕНЦИИ: ОПК-7
ПОКАЗАТЕЛИ, КРИТЕРИИ ОЦЕНИВАНИЯ (планируемые результаты обучения)
ЗНАЕТ: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;
УМЕЕТ: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;
ВЛАДЕЕТ:методами управления и регулирования правовых отношений отрасли инфокоммуникаций в рыночной среде;
• методами управления и регулирования правовых отношений отрасли инфокоммуникаций в рыночной среде;

КОД КОМПЕТЕНЦИИ: ОПК-8
ПОКАЗАТЕЛИ, КРИТЕРИИ ОЦЕНИВАНИЯ (планируемые результаты обучения)
ЗНАЕТ:основные природные и техносферные опасности;
УМЕЕТ:выбирать методы защиты от опасностей;
ВЛАДЕЕТ:методами защиты в чрезвычайных ситуациях, методами оказания первой помощи; умением разрабатывать и применять мероприятия по охране труда и;

КОД КОМПЕТЕНЦИИ: ПК-1
ПОКАЗАТЕЛИ, КРИТЕРИИ ОЦЕНИВАНИЯ (планируемые результаты обучения)
ЗНАЕТ: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;
УМЕЕТ:Программно реализовать алгоритмы безопасности;
формулировать научно обоснованную проблему;;
ВЛАДЕЕТ:Методами организации защиты объекта от внешних угроз и технологиями защиты информации;
навыками самостоятельного научного поиска, реализуемыми при написании текста своей магистерской диссертации;;

КОД КОМПЕТЕНЦИИ: ПК-2
ПОКАЗАТЕЛИ, КРИТЕРИИ ОЦЕНИВАНИЯ (планируемые результаты обучения)
ЗНАЕТ: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;
УМЕЕТ: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;
ВЛАДЕЕТ:- 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;

КОД КОМПЕТЕНЦИИ: ПК-3
ПОКАЗАТЕЛИ, КРИТЕРИИ ОЦЕНИВАНИЯ (планируемые результаты обучения)
ЗНАЕТ: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 эффектив-ности 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;
УМЕЕТ:-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;
ВЛАДЕЕТ: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;

КОД КОМПЕТЕНЦИИ: ПК-4
ПОКАЗАТЕЛИ, КРИТЕРИИ ОЦЕНИВАНИЯ (планируемые результаты обучения)
ЗНАЕТ:основные нормативные правовые документы, международные и отечественные стандарты в области информационных систем (ИС) и технологий;;
УМЕЕТ:пользоваться основными нормативными документами РФ;
ВЛАДЕЕТ:навыками поиска необходимых нормативных и законодательных документов и навыками работы с ними в области ИС;

КОД КОМПЕТЕНЦИИ: ПК-5
ПОКАЗАТЕЛИ, КРИТЕРИИ ОЦЕНИВАНИЯ (планируемые результаты обучения)
ЗНАЕТ: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 эффектив-ности 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;
УМЕЕТ: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;
ВЛАДЕЕТ: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;

КОД КОМПЕТЕНЦИИ: ПК-6
ПОКАЗАТЕЛИ, КРИТЕРИИ ОЦЕНИВАНИЯ (планируемые результаты обучения)
ЗНАЕТ:методы проведения научных исследований и расчетов;
методы проведения научных исследований и расчетов;;
УМЕЕТ:вести библиографическую работу с привлечением современных информационных технологий;
вести библиографическую работу с привлечением современных информационных технологий;;
ВЛАДЕЕТ:методами и инструментами моделирования при исследовании систем и сетей инфокоммуникаций;
методами и инструментами моделирования при исследовании систем и сетей инфокоммуникаций.;

КОД КОМПЕТЕНЦИИ: ПК-7
ПОКАЗАТЕЛИ, КРИТЕРИИ ОЦЕНИВАНИЯ (планируемые результаты обучения)
ЗНАЕТ:Законодательную основу и ограничения, регулирующие санкционированное проведение аудита и теста на проникновение;
понятие, сущность, цели и задачи комплексной системы защиты информации;
УМЕЕТ: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;
ВЛАДЕЕТ: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;

КОД КОМПЕТЕНЦИИ: ПК-8
ПОКАЗАТЕЛИ, КРИТЕРИИ ОЦЕНИВАНИЯ (планируемые результаты обучения)
ЗНАЕТ:- 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;
УМЕЕТ:- 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;
ВЛАДЕЕТ:- 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;

КОД КОМПЕТЕНЦИИ: ПК-9
ПОКАЗАТЕЛИ, КРИТЕРИИ ОЦЕНИВАНИЯ (планируемые результаты обучения)
ЗНАЕТ:Законодательную основу и ограничения, регулирующие санкционированное проведение аудита и теста на проникновение;
УМЕЕТ:Составлять план аудита и тестирования на проникновения в зависимости от требуемого уровня анализа и используемых механизмов;
ВЛАДЕЕТ:Основными механизмами проведения теста на проникновение и программным обеспечением, используемым для проведения этого теста;

КОД КОМПЕТЕНЦИИ: ПК-10
ПОКАЗАТЕЛИ, КРИТЕРИИ ОЦЕНИВАНИЯ (планируемые результаты обучения)
ЗНАЕТ: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;
УМЕЕТ: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;
ВЛАДЕЕТ:Знаниями о правовом обеспечении защиты информации;
навыками лицензирования программного обеспечения;
• методами управления и регулирования правовых отношений отрасли инфокоммуникаций в рыночной среде;

КОД КОМПЕТЕНЦИИ: ПК-11
ПОКАЗАТЕЛИ, КРИТЕРИИ ОЦЕНИВАНИЯ (планируемые результаты обучения)
ЗНАЕТ:методы и средства контроля качества продукции, организацию и технологию стандартизации и сертификации продукции;
УМЕЕТ:примерять средства измерений для контроля качества продукции и технологических процессов;
ВЛАДЕЕТ:средствами и методами повышения безопасности и экологичности технических средств и технологических процессов;

КОД КОМПЕТЕНЦИИ: ПК-12
ПОКАЗАТЕЛИ, КРИТЕРИИ ОЦЕНИВАНИЯ (планируемые результаты обучения)
ЗНАЕТ: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;
УМЕЕТ: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;
ВЛАДЕЕТ:методами и инструментами моделирования при исследовании систем и сетей инфокоммуникаций.;

КОД КОМПЕТЕНЦИИ: ПК-13
ПОКАЗАТЕЛИ, КРИТЕРИИ ОЦЕНИВАНИЯ (планируемые результаты обучения)
ЗНАЕТ:требования режима защиты информации ограниченного доступа;
УМЕЕТ:разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности телекоммуникационных систем;
ВЛАДЕЕТ:знаниями о режимах защиты информации ограниченного доступа;

КОД КОМПЕТЕНЦИИ: ПК-14
ПОКАЗАТЕЛИ, КРИТЕРИИ ОЦЕНИВАНИЯ (планируемые результаты обучения)
ЗНАЕТ:- 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;
УМЕЕТ:- 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;;
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;
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;
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;
ВЛАДЕЕТ: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;

КОД КОМПЕТЕНЦИИ: ПК-15
ПОКАЗАТЕЛИ, КРИТЕРИИ ОЦЕНИВАНИЯ (планируемые результаты обучения)
ЗНАЕТ: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;
УМЕЕТ:- 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;
ВЛАДЕЕТ: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;

КОД КОМПЕТЕНЦИИ: ПСК-12.1
ПОКАЗАТЕЛИ, КРИТЕРИИ ОЦЕНИВАНИЯ (планируемые результаты обучения)
ЗНАЕТ: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;
УМЕЕТ: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;
ВЛАДЕЕТ: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;

КОД КОМПЕТЕНЦИИ: ПСК-12.2
ПОКАЗАТЕЛИ, КРИТЕРИИ ОЦЕНИВАНИЯ (планируемые результаты обучения)
ЗНАЕТ:высокоуровневые средства, для эффективного проектирования;
УМЕЕТ:выбирать и (или) строить адекватные, математические и алгоритмические модели;
ВЛАДЕЕТ:способностью обоснованно выбирать и (или) строить адекватные, математические и алгоритмические модели;

КОД КОМПЕТЕНЦИИ: ПСК-12.3
ПОКАЗАТЕЛИ, КРИТЕРИИ ОЦЕНИВАНИЯ (планируемые результаты обучения)
ЗНАЕТ:математический аппарат используемый при построении телекоммуникационных систем;
принципы построения высокоэффективных телекоммуникационных систем;
УМЕЕТ:анализировать телекоммуникационные сигналы и системы;
управлять поведением телекоммуникационных систем информационного взаимодействия и систем;
ВЛАДЕЕТ:методами математического анализа и расчета сигналов и систем;
способностью обоснованно выбирать и применять адекватные методы кодирования;

КОД КОМПЕТЕНЦИИ: ПСК-12.4
ПОКАЗАТЕЛИ, КРИТЕРИИ ОЦЕНИВАНИЯ (планируемые результаты обучения)
ЗНАЕТ:Стек протоколов IPSEC .Методы защиты сетевых устройств и систем;
УМЕЕТ:разрабатывать комплексную политику сетевой безопасности .конфигурировать систему предотвращения вторжений (IPS);
ВЛАДЕЕТ:навыками настройки статических (site-to-site) VPN соединений .навыками конфигурирования устройств локальной сети для контроля доступа;

КОД КОМПЕТЕНЦИИ: ПСК-12.5
ПОКАЗАТЕЛИ, КРИТЕРИИ ОЦЕНИВАНИЯ (планируемые результаты обучения)
ЗНАЕТ:работу телекоммуникационных систем информационного взаимодействия;
УМЕЕТ:оценивать уровень защиты кода от исследования и поиска несанкционированного или вредоносного вмешательства;
ВЛАДЕЕТ:способностью применять стандартные средства для анализа программного кода;

Критерии, указанные в таблице 2, разработаны с учетом требований ФГОС ВО к конечным результатам обучения и создают основу для выявления уровня сформированности компетенций: минимального, базового или высокого.

3.2.Стандартные критерии оценивания.

Показатели и критерии оценивания компетенций применяются в отношении отчетной документации по практике, а также устного ответа обучающегося.

Состав отчетной документации по практике:

- дневник практики (ведется по форме Направления-задания согласно Положению о практиках в СПБГУТ);
- отчет по практике (в том числе презентация, публикации);
- отзыв с места прохождения практики.

Отчетная документация по практике должна соответствовать стандартным критериям, определенным в Положении о практиках в СПБГУТ.

Критерии оценки устного ответа в ходе собеседования при защите отчета по практике:

- логика при изложении содержания ответа на вопрос, выявленные знания соответствуют объему и глубине их раскрытия в источнике;
- использование научной терминологии в контексте ответа;
- объяснение причинно-следственных и функциональных связей;
- умение оценивать действия субъектов социальной жизни, формулировать собственные суждения и аргументы по определенным проблемам;
- эмоциональное богатство речи, образное и яркое выражение мыслей.

Критерии оценки презентации:

- содержание раскрывает тему;
- логичность изложения материала при раскрытии темы, наличие выводов;
- оформление презентации соответствует установленным требованиям;
- качество выступления автора: свободное владение материалом; текст зачитывает; кратко и точно отвечает на вопросы и т.д.;

Требования к составлению презентации:

- титульный слайд (название работы, ФИО автора, ФИО руководителя);
- цель выполнения работы и задачи;
- содержание работы (излагается на нескольких слайдах);
- заключение, выводы по работе;
- использованные библиографические источники;
- заключительный слайд.

При составлении презентации необходимо рассчитывать количество слайдов в соответствии с установленным регламентом времени на выступление и на обсуждение материалов презентации.

Критерии оценки ответа за зачет:

Для зачета в устном виде употребимы критерии оценки устного ответа в ходе собеседования (см. выше)

Порядок применения критериев оценки конкретизирован ниже, в разделе 4, содержащем оценочные средства для текущего контроля успеваемости и для проведения промежуточной аттестации студентов по данной дисциплине.

3.3.Описание шкал оценивания.

Шкала оценивания необходима для соотнесения результатов оценивания и этапов формирования компетенций в процессе прохождения практики (таблица 3).

Таблица 3

Показатели оценивания	**Описание в соответствии с критериями оценивания, приведенными в таблице 3**	**Оценка знаний, умений, навыков и опыта**	**Академическая оценка**	
			по бальной шкале	**по дихотомической шкале**
Высокий уровень освоения	Демонстрирует полное понимание проблемы. Требования по всем критериям выполнены	«очень высокая», «высокая»	«отлично»	«зачтено»
Базовый уровень освоения	Демонстрирует значительное понимание проблемы. Требования по всем критериям выполнены	«достаточно высокая», «выше средней», «базовая»	«хорошо»	«зачтено»
Минимальный уровень освоения	Демонстрирует частичное понимание проблемы. Требования по большинству критериев выполнены	«средняя», «ниже средней», «низкая», «минимальная»	«удовлетворительно»	«зачтено»
Недостаточный уровень освоения	Демонстрирует небольшое понимание проблемы. Требования по многим критериям не выполнены	«очень низкая», «примитивная»	«неудовлетворительно»	«незачтено»

При проведении промежуточной аттестации студентов по данной дисциплине в форме зачета используется дихотомическая шкала оценивания. При использовании других шкал преподавателем вводится соответствующая шкала оценивания дополнительно к пятибалльной или дихотомической.

Условием получения зачета по практике является полностью выполненное индивидуальное задание, что должно быть отражено в отчетной документации по практике и исчерпывающие ответы на вопросы, которые содержатся в перечне примерных вопросов для подготовки к промежуточной аттестации по итогам практики.

4. Типовые контрольные задания, иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Аттестация по итогам практики осуществляется после сдачи документов по практике на кафедру и фактической защиты отчета на основе оценки решения

студентом задач практики, отзыва руководителей практики об уровне знаний и квалификации студента. По результатам аттестации выставляется зачет.

При оценке итогов работы студента на практике, учитываются содержание и правильность оформления студентом дневника и отчета по практике, отзывы руководителей практики от организации - места прохождения практики и кафедры, качество ответов на вопросы в ходе защиты отчета.

4.1.Оценочные средства текущего контроля успеваемости

Примерная тематика индивидуальных заданий по практике

Подготовка материалов и проведение практического эксперимента для выпускной квалификационной работы

Перечень вопросов по оценке сформированности компетенций образовательной программы приведен в Приложении 1.

Дневник практики

Учет работы, в том числе и самостоятельной, выполненной в ходе практики ведется каждым студентом в дневнике практики. Дневник практики (бланк «Направление на практику») ведется по форме согласно Положению о практиках в СПбГУТ .

Дневник практики заполняется по каждому разделу (этапу) практики. Записи в дневнике должны содержать краткое описание выполненной работы с анализами и выводами, а также данные, характеризующие ее объем. Дневники проверяются и подписываются руководителями практики. По завершении каждого раздела (этапа) практики студент представляет соответствующие виды отчетности, содержание и характер которых должны соответствовать программе практики.

Отчет по практике

В период прохождения практики каждым студентом по мере накопления материала составляется отчет, в котором должны найти отражение все разделы (этапы) практики, предусмотренные программой, включая индивидуальные задания. Отчет является обязательным для всех студентов. При его оформлении следует соблюдать требования ГОСТ.

Отчет должен содержать информационный и практический материал, собранный студентом во время практики, а также перечисление практических умений и навыков, полученных студентом. В отчете также может найти отражение работа, выполненная студентом по заданию руководителей практики (помимо учебных заданий).

4.2.Оценочные средства промежуточной аттестации

Отзыв с места прохождения практики

Отзыв с места прохождения практики оформляется в направлении–задании на практику в разделе характеристика студента-практиканта и включает оценку руководителя от базы практики.

Отзыв и направление-задание должны быть проверены и подписаны руководителем практики от базы практики. В отзыве руководитель дает письменное заключение о знаниях и навыках, приобретенные студентом за время прохождения производственной практики и оценивает проделанную работу студента.

Отзыв включает в себя заключение о работе студента за период прохождения практики: теоретическая подготовленность, технические навыки, результаты выполнения индивидуальных заданий и программы практики в целом, сведения о трудовой дисциплине, отношении к работе, участию в общественной жизни.

Перечень примерных вопросов для промежуточной аттестации по итогам практики

Представленный Перечень теоретических вопросов (заданий) является основой для генерирования вопросов к зачету.

5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и/или опыта деятельности, характеризующих этапы формирования компетенций

Основным руководящим документом, в соответствии с которым проводится практика, является Программа практики. На основании Программы практики определяется содержание практики, разрабатывается календарный план ее прохождения, ставятся индивидуальные задачи на период прохождения практики, заполняется дневник прохождения практики и составляется Отчет по практике. Состав методических материалов, определяющих процедуры оценивания, определяется рабочей программой практики с учетом цели ее проведения. Учебная практика проводится в целях получения первичных профессиональных умений и навыков. Производственная практика проводится в целях получения профессиональных умений и опыта профессиональной деятельности. В случае, если ФГОС ВО по соответствующему направлению подготовки предусмотрена защита выпускной квалификационной работы, то в составе производственной практики обязательно проводится преддипломная практика.

5.1.Методические материалы для текущего контроля успеваемости

В период практики студент должен проявить себя как начинающий специалист, обладающий высокими моральными качествами, общественной активностью. Он должен быть примером организованности, дисциплинированности и трудолюбия, должен стремиться показать свою профессиональную компетентность, активно участвовать в жизни коллектива.

Отсутствие практиканта на закрепленном рабочем месте считается прогулом. Если прогулы составляют более 30% рабочего времени, практика не засчитывается.

По итогам практики студент представляет руководителю отчетную документацию: Дневник практики; Отзыв от принимающей организации о прохождении практики; Отчет по практике.

При оценке итогов работы студента на практике, учитываются содержание и правильность оформления им дневника и отчета по практике, степень выполнения программы и индивидуального задания, отзывы руководителей практики от организации - места прохождения практики и кафедры, качество ответов на вопросы в ходе защиты отчета.

Дневник практики составлен по форме, установленной в СПбГУТ.

Рекомендации по заполнению дневника практики.

Требования к структуре Отчета по практике.

5.2.Методические материалы для промежуточной аттестации

Форма промежуточной аттестации по дисциплине – зачет

Форма проведения зачета: смешанная

Аттестация по итогам практики осуществляется после сдачи документов по практике на кафедру и фактической защиты отчета на основе оценки решения студентом задач практики, отзыва руководителей практики об уровне знаний и квалификации обучающегося. По результатам аттестации выставляется дифференцированный зачет.

- оценка «отлично» - выставляется, если студент своевременно в установленные сроки представил на кафедру оформленные в соответствии с требованиями отзыв, дневник, отчет о прохождении практики; имеет отличную характеристику (отзыв) от руководителя предприятия - базы практики; изложил в отчете в полном объеме вопросы по всем разделам практики; во время защиты отчета правильно ответил на все вопросы руководителя практики от университета.;
- оценка «хорошо» - выставляется, если своевременно в установленные сроки студент представил на кафедру отзыв, дневник, отчет о прохождении практики; имеет отличную характеристику (отзыв) от руководителя предприятия - базы практики; в отчете в полном объеме осветил вопросы по разделам практики; но получил незначительные замечания по оформлению отчетных документов по практике или во время защиты отчета ответил не на все вопросы руководителя практики от университета;
- оценка «удовлетворительно» - выставляется, если студент своевременно в установленные сроки представил на кафедру отзыв, дневник, отчет о прохождении практики; но получил существенные замечания по оформлению отчетных документов по практике или в отчете не в полном объеме осветил вопросы по разделам практики; или во время защиты отчета ответил не на все вопросы руководителя практики от университета;
- оценка «неудовлетворительно» - выставляется студенту, отсутствующему на закрепленном рабочем месте базы практики или не выполнившему программу практики, или получившему отрицательный отзыв о работе, или ответившему неверно на вопросы преподавателя при защите отчета.

В случае невыполнения предъявляемых требований практикант может быть отстранен от прохождения практики. Студент, отстраненный от практики или работа которого на практике признана неудовлетворительной, считается не выполнившим учебный план данного семестра.

Нарушением дисциплины и невыполнением учебного плана считается несвоевременная сдача обучающимися документации по практике. Студенты, не выполнившие программу практики, получившие отрицательный отзыв о работе или неудовлетворительную оценку при защите отчета, отчисляются за академическую неуспеваемость.

В случае уважительной причины студенты, не получившие зачет по практике, направляются на повторное прохождение практики.