МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
Северо-Кавказский филиал
ордена Трудового Красного Знамени федерального государственного
бюджетного образовательного учреждения высшего образования
«Московский технический университет связи и информатики»

УТВЕРЖДАЮ
Зам. директора по УВР
_____
«14» 05 2022 г.

Производственная (технологическая) практика
Б1.О.02(П)
рабочая программа

Кафедра: «Инфокоммуникационные технологии и системы связи»

Направление подготовки: **11.03.02 Инфокоммуникационные технологии и системы связи**

Профиль: **Защищенные инфокоммуникационные системы**

Формы обучения: **Очная, заочная**

Объем и структура производственной практики по семестрам для очной формы обучения (ОФО), курсам для заочной формы обучения (ЗФО)				
Вид учебной работы	ОФО		ЗФО	
	ЗЕ	часов	ЗЕ	часов
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	9 (6 недель)	324/6	9 (6 недель)	324/4
Контактная работа, в том числе (по семестрам, курсам):		2/6		2/4
Самостоятельная работа		322/6		322/4
Число зачетов с оценкой с разбивкой по семестрам (курсам)		1/6		1/4
Способы и формы проведения производственной практики				
Способ проведения	Стационарная Выездная		Стационарная Выездная	
Форма проведения	Дискретная		Дискретная	

Программу составил:
Зав. кафедрой ИТСС к.т.н., доцент Юхнов В.И.

Рецензент:
Ведущий научный сотрудник ФГУП «РНИИРС, д.т.н., доцент Елисеев А.В.

Рабочая программа
Производственная(технологическая) практика

Разработана в соответствии с ФГОС ВО
направления подготовки 11.03.02 ИНФОКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ И СИСТЕМЫ СВЯЗИ, утвержденным приказом Министерства образования и науки Российской Федерации от 19 сентября 2017 г. N 930.

.

Составлена на основании учебных планов
направления 11.03.02 Инфокоммуникационные технологии и системы связи профиль «Защищенные инфокоммуникационные системы», одобренных Учёным советом СКФ МТУСИ, протокол № 9 от 22.04.2024, и утвержденных директором СКФ МТУСИ 22.04.2024 г

Рассмотрена и одобрена на заседании кафедры
«Инфокоммуникационные технологии и системы связи»

Протокол от «20» 05 2024 г. № 10

Зав. кафедрой _____Юхнов В.И.

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР ________________
«___» _______ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры

«Инфокоммуникационные технологии и системы связи»

Протокол от «___» _______ 20__ г. № ____
Зав. кафедрой _____________________

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР ________________
«___» _______ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры
«Инфокоммуникационные технологии и системы связи»

Протокол от «___» _______ 20__ г. № ____
Зав. кафедрой _____________________

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР ________________
«___» _______ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры
«Инфокоммуникационные технологии и системы связи»

Протокол от «___» _______ 20__ г. № ____
Зав. кафедрой _____________________

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР ________________
«___» _______ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры
«Инфокоммуникационные технологии и системы связи»

Протокол от «___» _______ 20__ г. № ____
Зав. кафедрой _____________________

1. Цели производственной (технологической) практики

Целями производственной (технологической) практики являются систематизация теоретических знаний, полученных в процессе обучения, приобретение и совершенствование профессиональных умений и навыков в области профессиональной деятельности.

2. Планируемые результаты обучения

Изучение дисциплины направлено на формирование у выпускника способности решать задачи в соответствии с профессиональной технологической деятельностью.

Результатом освоения дисциплины являются сформированные у выпускника следующие компетенции:

ПК-1: Способен обеспечить защиту от несанкционированного доступа сооружений и средств связи сетей электросвязи
Знать (Необходимые знания):
методы контроля функционирования СССЭ, их защищенности от НСД; принципы построения современных сетей электросвязи, математические модели каналов связи, виды модуляции сигналов; функциональное назначение и основные характеристики средств контроля функционирования СССЭ, их защищенности от НСД; организация и содержание мониторинга функционирования СССЭ, их защищенности от НСД; возможные источники и технические каналы утечки информации; нормативные правовые акты в области связи и защиты информации.
Уметь (Необходимые умения):
использовать средства мониторинга работоспособности и эффективности применяемых программных, программно-аппаратных (в том числе криптографических) и технических средств защиты СССЭ от НСД; проводить контроль функционирования СССЭ, их защищенности от НСД; определять технические характеристики СССЭ, их защищенности от НСД. оценивать помехоустойчивость и эффективность сетей электросвязи при передаче трафика, оптимизировать их параметры; осуществлять проверки СССЭ, программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД на соответствие заданным требованиям; проводить документационное обеспечение функционирования СССЭ, их защищенности от НСД.
Владеть (Трудовые действия):
средствами анализа функциональности СССЭ, защищенности от НСД сооружений и СССЭ; умением контролировать ь целостности сооружений и СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД; составлением отчетов по результатам проверок, в том числе выявление инцидентов, которые могут привести к сбоям или нарушению функционирования или возникновению угроз безопасности информации, циркулирующей в СССЭ
ПК-2: Способен разрабатывать, проектировать, внедрять и эксплуатировать объекты и системы связи, телекоммуникационные системы, системы подвижной связи различного назначения

Знать (Необходимые знания):
Принципы работы, состав и основные характеристики монтируемого оборудования; Принципы построения спутниковых и наземных систем связи; Стандарты и протоколы информационных сигналов, видов сигнализации, назначения интерфейсов Технологии монтажа оборудования связи (телекоммуникаций); Технологии выполнения работ по настройке, регулировке и испытаниям оборудования связи (телекоммуникаций); Схемы операционного контроля качества; Порядок приемки оборудования в эксплуатацию; Методики применения измерительного и тестового оборудования. Конструктивные особенности, принципиальные, монтажные и функциональные схемы монтируемого оборудования; Правила и инструкции по паспортизации оборудования; Правила эксплуатации измерительных приборов Действующие отраслевые нормативы, определяющие требования к параметрам работы оборудования, каналов и трактов; Методики проведения контроля проектных параметров и режимов работы оборудования
Уметь (Необходимые умения):
Проверять рабочую документацию на полноту содержания и комплектность; Выполнять работы по монтажу аппаратуры связи различного назначения; Пользоваться проектной и технической документацией на монтаж оборудования связи (телекоммуникаций) Проводить внешний осмотр поступившего для монтажа оборудования, кабелей на их соответствие сопроводительным документам; Тестировать оборудование и отрабатывать режимы работы оборудования Выбирать соответствующее тестовое и измерительное оборудование Использовать программное обеспечение оборудования при его настройке Анализировать полученные результаты; Проводить измерения параметров оборудования, каналов и трактов.
Владеть (Трудовые действия):
Проведением входного контроля оборудования; Разработкой программы пусконаладочных работ; Выполнением тестирования оборудования; Выполнением настройки, регулировки и испытаний оборудования связи (телекоммуникаций); Обеспечением строгого соблюдения технологии работ, своевременного выявления дефектов и их устранение; Подготовкой испытательного оборудования, измерительной аппаратуры, приспособлений; Отработкой режимов работы оборудования с выявлением оптимальных условий работы этого оборудования; Выполнением монтажа технологического оборудования, линейных сооружений, антенно-фидерных устройств (на участках высокой сложности); Контролем проектных параметров и режимов работы оборудования связи (телекоммуникаций); Составлением технического отчета
ПК-3: Способен выполнять работы по администрированию процесса управления

безопасностью сетевых устройств и программного обеспечения
Знать (Необходимые знания):
общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети; архитектуру аппаратных, программных и программно-аппаратных средств администрируемой сети; классификацию операционных систем согласно классам безопасности; средства защиты от несанкционированного доступа операционных систем и систем управления базами данных; инструкции по установке администрируемых сетевых устройств; инструкции по эксплуатации администрируемых сетевых устройств; инструкции по установке администрируемого программного обеспечения; инструкции по эксплуатации администрируемого программного обеспечения; протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем; модель ISO для управления сетевым трафиком; модели IEEE; защищенные протоколы управления; основные средства криптографии; регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе; требования охраны труда при работе с сетевой аппаратурой администрируемой сети.
Уметь (Необходимые умения):
выяснять приемлемые для пользователей параметры работы сети в условиях нормальной (обычной) работы (базовые параметры); применять аппаратные средства защиты сетевых устройств от несанкционированного доступа; применять программные средства защиты сетевых устройств от несанкционированного доступа; применять программно-аппаратные средства защиты сетевых устройств от несанкционированного доступа пользоваться нормативно-технической документацией в области инфокоммуникационных технологий; настраивать параметры современных программно-аппаратных межсетевых экранов; сегментировать элементы администрируемой сети; работать с контрольно-измерительными аппаратными и программными средствами
Владеть (Трудовые действия):
планированием защиты приложений от несанкционированного доступа оценкой безопасности и защиты приложений от несанкционированного доступа планированием защиты операционных систем от несанкционированного доступа оценкой защиты операционных систем от несанкционированного доступа установкой специализированных программных средств защиты сетевых устройств администрируемой сети от несанкционированного доступа установкой межсетевых экранов, гибких коммутаторов, средств предотвращения атак виртуальной частной сети

3. Место производственной (технологической) практики в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Производственная практика является логическим продолжением изучения дисциплин Б1.О.24 Основы информационной безопасности Б1.В.07 Линии радиосвязи и методы их защиты Б1.В.09 Направляющие телекоммуникационные среды и методы их защиты знание которых в объеме требований образовательной программы является необходимым.
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Прохождение производственной практики необходимо для успешного прохождения преддипломной практики, а также написания выпускной квалификационной работы.

4. Структура и содержание практики

4.1 Очная форма обучения, 4 г., заочная форма обучения, 4г.8 мес. (всего 324 часа)

Код зан.	Тема и краткое содержание работы	Кол. часов	Компе-тенции	УМИО
Модуль 1				
1.1	Инструктаж по ПМБ. Изучение требований правил и мер безопасности, установленных в компании и непосредственно на рабочем месте.	8	ПК-1, ПК-2, ПК-3	Л1.1-Л1.3
1.2	Изучение требований основных ведомственных руководящих документов и документов Министерства связи в области деятельности компании связи.	20	ПК-1, ПК-2, ПК-3	Л2.1-Л2.10
1.3	Рассмотрение штатной структуры организации и своего места в ней. Анализ перспектив развития организации.	20	ПК-1, ПК-2, ПК-3	Л1.4
1.4	Изучение функциональных обязанностей должностного лица, в качестве которого проходит практика, и ознакомление с организацией рабочего места.	20	ПК-1, ПК-2, ПК-3	Л1.4
1.5	Изучение правил и периодичности проведения технического обслуживания оборудования, а также правил проверки работоспособности оборудования и методов устранения неисправностей.	20	ПК-1, ПК-2, ПК-3	Л1.1
1.6	Изучение требований по размещению криптографического оборудования	20	ПК-1, ПК-2, ПК-3	Л1.1-Л1.4
1.7	Рассмотрение вопросов применения дополнительного оборудования для информационной защиты телекоммуникационного оборудования	20	ПК-1, ПК-2, ПК-3	Л1.1-Л1.4
1.8	Исполнение обязанностей должностного лица организации по назначенной должности, эксплуатация закреплённого оборудования. Деловое общение с сотрудниками компании и её клиентами.	20	ПК-1, ПК-2, ПК-3	Л1.1-Л1.4
1.9	Рассмотрение общей схемы сети (участка сети), состава оборудования связи и правил его эксплуатации.	20	ПК-1, ПК-2, ПК-3	Л1.2-Л1.4
1.10	Рассмотрение текущих и перспективных потребностей населения в услугах, предоставляемых по средствам телекоммуникационных сетей.	20	ПК-1, ПК-2, ПК-3	Л1.4
1.11	Определение возможных перспективных направлений для развития (модернизации) сетевой структуры организации с целью обеспечения перспективных потребностей населения.	20	ПК-1, ПК-2, ПК-3	Л1.4
1.12	Изучение используемой, в рассматриваемой сети, технологии передачи. Особенности работы оборудования.	20	ПК-1, ПК-2, ПК-3	Л1.1, Л1.4
1.13	Определение необходимости модернизации оборудования связи, исходя из сроков эксплуатации и технического состояния.	20	ПК-1, ПК-2, ПК-3	Л1.1-Л1.4
1.14	Подготовка технической документации и необходимых заявок на ремонт или замену оборудования.	20	ПК-1, ПК-2,	Л1.1-Л1.4

			ПК-3	
1.15	Изучение правил организации рабочих мест и оснащения их техническим оборудованием.	20	ПК-1, ПК-2, ПК-3	Л1.4
1.16	Обобщение результатов работы. Написание отчёта по производственной практике и получение отзыва о работе во время практики.	20	ПК-1, ПК-2, ПК-3	Л1.1-Л1.3, Л3.1
1.17	Подведение итогов практики, отчёт перед руководителем от предприятия. Получение отзыва о работе.	14	ПК-1, ПК-2, ПК-3	Л3.1
Зачёт с оценкой – 2 час				
Итого – 324 часа				

4.2 Формы отчетности по практике

Формами отчетности студентов по практике являются:

1) ***Заполненный дневник с отзывом руководителя практики.***

Содержание дневника должно соответствовать индивидуальному заданию и плану производственной практики. Подписи представителя организации о прибытии на практику и убытии с неё, а также подпись руководителя практики от предприятия под его отзывом должны быть заверены печатью организации, в которой проводилась практика.

2) ***Отчет по практике.***

Отчет по практике оформляется отдельным документом в печатном виде на бумаге формата А4. Он должен содержать:

– титульный лист (образец приведен на сайте филиала);

– содержание практики (в соответствии с Программой производственной практики);

– краткие теоретические сведения и свидетельства выполнения Плана и Программы практики (скриншоты, фотографии оборудования, должностные инструкции и т.д.), а также анализ технологий передачи данных и другие общие вопросы, относящиеся к выполнению ВКР;

– перечень и обзор использованных студентом информационных источников и нормативных документов;

– выводы и предложения студента по практике.

Отчет по практике подписывается студентом, проверяется и визируется руководителем практики от организации и руководителем практики от института. Защита отчетов производится в соответствии с установленным графиком защиты отчетов. Нарушение сроков прохождения практики и сроков защиты считается невыполнением учебного плана. По результатам защиты отчетов по практике в институте студенту выставляется оценка.

3) Ответы на контрольные вопросы и выполнение задач.

5. Учебно-методическое и информационное обеспечение дисциплины

7.1. Рекомендуемая литература				
7.1.1. Основная литература				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**
Л1.1		Эксплуатационная документация на используемое оборудование связи.	Производ-ль оборудования.	
Л1.2		Нормативные документы по организации и контролю обеспечения безопасной эксплуатации оборудования связи.	Организация	
Л1.3		Нормативные документы по организации и техническому обслуживанию оборудования связи.	Производ-ль оборудования.	
Л1.4		Сборник документов по организации работы компании.	Организация	
7.1.2. Дополнительная литература				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**
Л2.1		Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 21.07.2014) "О персональных данных" (с изм. и доп., вступ. в силу с 01.09.2015)		Э1
Л2.2		Федеральный закон от 06.04.2011 N 63-ФЗ (ред. от 30.12.2015) "Об электронной подписи"		Э2
Л2.3		Федеральный закон от 07.07.2003 N 126-ФЗ (ред. от 13.07.2015) "О связи" (с изм. и доп., вступ. в силу с 10.01.2016)		Э3
Л2.4		Федеральный закон от 17 июля 1999 г. N 176-ФЗ "О почтовой связи" (7 июля 2003 г., 22 августа, 29 декабря 2004 г., 26 июня 2007 г., 14, 23 июля 2008 г., 28 июня 2009 г., 6 декабря 2011 г., 2 марта 2016 г.)		Э4
Л2.5		Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 10.01.2016)		Э5
Л2.6		Закон РФ от 21 июля 1993 г. N 5485-I "О государственной тайне" (с изменениями и дополнениями от 6 октября 1997 г., 30 июня, 11 ноября 2003 г., 29 июня, 22 августа 2004 г., 1 декабря 2007 г., 18 июля 2009 г., 15 ноября 2010 г., 18, 19 июля, 8 ноября 2011 г., 21 декабря 2013 г., 8 марта 2015 г.)		Э6
Л2.7		Указ Президента РФ от 17 марта 2008 г. N 351 "О мерах по обеспечению		Э7

		информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена" (с изменениями и дополнениями от 21 октября 2008 г., 14 января 2011 г., 1, 25 июля 2014 г., 22 мая 2015 г.		
Л2.8		Приказ Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"		Э8
Л2.9		ГОСТ 34.936-91 Информационная технология. Локальные вычислительные сети. Определение услуг уровня управления доступом к среде		Э9
Л2.10		ГОСТ Р 53724-2009 Качество услуг связи. Общие положения		Э10

7.1.3. Учебно-методическое обеспечение для самостоятельной работы обучающихся

Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л3.1	Сосновский И.А.	Методические указания по проведению Производственной (преддипломной) практики для студентов по направлению подготовки 11.03.02	РнД: СКФ МТУСИ, 2022	Э11

7.2. Электронные образовательные ресурсы

Э1	http://www.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=178749
Э2	http://www.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=191956
Э3	http://www.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=201564
Э4	http://www.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=201192
Э5	http://ivo.garant.ru/#/document/12148555/paragraph/3471:2
Э6	http://ivo.garant.ru/#/document/10102673/paragraph/51952:4
Э7	http://ivo.garant.ru/#/document/192944/paragraph/8911:2
Э8	http://ivo.garant.ru/#/document/70391358/paragraph/1:4
Э9	http://www.infosait.ru/Pages_gost/19099.htm
Э10	http://docs.cntd.ru/document/gost-r-53724-2009
Э11	http://www.skf-mtusi.ru/?page_id=659

7.3. Программное обеспечение

П.1	OS Windows
П.2	Пакет Microsoft Office

6. Материально-техническое обеспечение дисциплины

Производственная (технологическая) практика организуется на предприятиях связи или в организациях, предоставляющих различные виды услуг связи. Возможно проведение практики на предприятиях, обладающих собственной развитой корпоративной сетью, на должностях, связанных с её эксплуатацией.

В перечисленных организациях должен находиться ряд оборудования связи, позволяющий получить опыт работы по его эксплуатации. К такому оборудованию относятся:

– защита терминальных сессий при использовании “тонких клиентов”;

– контроль утечек конфиденциальной информации – теперь СЗИ обеспечивает возможность теневого копирования при отчуждении конфиденциальной информации;

– универсальный контроль печати – вывод грифа конфиденциальности на документы, распечатываемые из любого приложения;

– разграничение доступа к принтерам - возможность печати конфиденциальных документов только на специально выделенных для этого принтерах;

– автоматическая конфигурация системы полномочного доступа;

– удаленное управление локальными политиками безопасности и состоянием защитных систем СЗИ с рабочего места администратора.

Дополнения и изменения к рабочей программе практики