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
_____ А.Г. Жуковский
«29» 08 2022 г.

Производственная (эксплуатационная) практика Б1.В.02(П)
рабочая программа дисциплины

Кафедра: Инфокоммуникационные технологии и системы связи
Направление подготовки: **10.03.01 Информационная безопасность**
Профиль: **Безопасность компьютерных систем**
Формы обучения: **очная**

Распределение часов дисциплины по семестрам (для очной формы обучения), курсам (для заочной формы обучения)

Вид учебной работы	ОФ		ЗФ	
	ЗЕ	часов	ЗЕ	часов
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	6	216/6 сем		
Контактная работа, в том числе (по семестрам, курсам):				
Лекции				
Лабораторных работ				
Практических занятий				
Семинаров				
Самостоятельная работа		216/6 сем		
Число зачетов с разбивкой по семестрам (курсам)		1/6		
Способы и формы проведения производственной практики				
Способ проведения	Стационарная Выездная			
Форма проведения	Дискретная			

Программу составил:
Доцент кафедры ИТСС к.т.н. Енгибарян И.А.

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

Рабочая программа дисциплины
«Производственная (эксплуатационная) практика»

Разработана в соответствии с ФГОС ВО:
направления подготовки 10.03.01 «Информационная безопасность», утвержденным приказом Министерства образования и науки Российской Федерации от 17 ноября 2020г. №1427.

Составлена на основании учебного плана
направления 10.03.01 «Информационная безопасность» профиля «Безопасность компьютерных систем», одобренного Учёным советом СКФ МТУСИ, протокол № 9 от 25.04.2022, и утвержденного директором СКФ МТУСИ 25.04.2022 г.

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

Протокол от «19» 08 2022г. № 1

Зав. кафедрой _____ В.И. Юхнов

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 изучения дисциплины

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

2. Планируемые результаты обучения

Изучение дисциплины направлено на формирование у выпускника способности решать профессиональные задачи в соответствии с ***эксплуатационным*** видом деятельности:

Результатом освоения дисциплины являются сформированные у выпускника следующие компетенции:

Компетенции выпускника, формируемые в результате освоения дисциплины (в части, обеспечиваемой дисциплиной)
ПК-2: Администрирование программно-аппаратных средств защиты информации в компьютерных сетях
Знать:
- принципы построения компьютерных сетей; - стек сетевых протоколов операционных систем; - стек протоколов сетевого оборудования; - порядок реализации методов и средств межсетевого экранирования; - принципы функционирования сетевых протоколов, включающих криптографические алгоритмы; - виды политик управления доступом и информационными потоками в компьютерных сетях; -источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению; - состав типовых конфигураций программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях; - методы измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации; - принципы работы и правила эксплуатации эксплуатируемых программно-аппаратных средств защиты информации; - программно-аппаратные средства и методы защиты информации в компьютерных сетях; - нормативные правовые акты в области защиты информации; - руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; - организационные меры по защите информации.
Уметь:
- оценивать угрозы безопасности информации в компьютерных сетях; - настраивать правила фильтрации пакетов в компьютерных сетях; - обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных сетях; - конфигурировать и контролировать корректность настройки программно-аппаратных средств защиты информации в компьютерных сетях; - выбирать режимы работы программно-аппаратных средств защиты информации в компьютерных сетях; - проводить мониторинг функционирования программно-аппаратных средств защиты информации в компьютерных сетях; - производить анализ эффективности программно-аппаратных средств защиты информации в компьютерных сетях; - оценивать оптимальность выбора программно-аппаратных средств защиты информации и их

режимов функционирования в компьютерных сетях.
Владеть:
- определением состава применяемых программно-аппаратных средств защиты информации в компьютерных сетях; - разработкой порядка применения программно-аппаратных средств защиты информации в компьютерных сетях; - формированием шаблонов конфигурации программно-аппаратных средств защиты информации в компьютерных сетях; - настройкой программных и аппаратных средств построения компьютерных сетей, использующих криптографическую защиту информации; - управлением функционированием программно-аппаратных средств защиты информации в компьютерных сетях; - контролем корректности функционирования программно-аппаратных средств защиты информации в компьютерных сетях; - управлением средствами межсетевого экранирования в компьютерных сетях в соответствии с действующими требованиями.
ПК-3: Администрирование средств защиты информации прикладного и системного программного обеспечения
Знать:
- архитектуру подсистем защиты информации в операционных системах; - принципы построения систем управления базами данных; - основные средства и методы анализа программных реализаций; - принципы построения антивирусного программного обеспечения; - виды политик управления доступом и информационными потоками применительно к прикладному программному обеспечению; - источники угроз информационной безопасности программного обеспечения и меры по их предотвращению; - уязвимости используемого программного обеспечения и методы их эксплуатации; - виды и формы функционирования вредоносного программного обеспечения; - характерные признаки наличия вредоносного программного обеспечения; - средства и методы обнаружения ранее неизвестного вредоносного программного обеспечения; - принципы функционирования программных средств криптографической защиты информации; - порядок обеспечения безопасности информации при эксплуатации программного обеспечения; - нормативные правовые акты в области защиты информации; - руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; - организационные меры по защите информации.
Уметь:
- анализировать угрозы безопасности информации программного обеспечения; - формулировать правила безопасной эксплуатации программного обеспечения; - обосновывать правила безопасной эксплуатации программного обеспечения; - анализировать функционирование программного обеспечения с целью определения возможного вредоносного воздействия; - производить проверку соответствия реальных характеристик программно-аппаратных средств защиты информации, заявленным в их технической документации; - осуществлять мероприятия по противодействию угрозам безопасности информации, возникающим при эксплуатации программного обеспечения; - определять порядок функционирования программного обеспечения с целью обеспечения

защиты информации; - анализировать эффективность сформулированных требований к встроенным средствам защиты информации программного обеспечения.
Владеть:
- определением порядка установки программного обеспечения с целью соблюдения требований по защите информации; - контролем над соблюдением требований по защите информации при установке программного обеспечения, включая антивирусное программное обеспечение; - формулированием требований к параметрам средств антивирусной защиты для корректной работы программного обеспечения; - выполнением работ по обнаружению вредоносного программного обеспечения; - ликвидацией обнаруженного вредоносного программного обеспечения и последствий его функционирования; - формулированием требований к встроенным средствам защиты информации программного обеспечения.

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

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Производственная (эксплуатационная) практика является логическим продолжением изучения дисциплин: Б1.О.33 Программно-аппаратные средства защиты информации Б1.О.34 Защита информации от утечки по техническим каналам Б1.О.40 Администрирование средств защиты информации в компьютерных системах и сетях
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Прохождение производственной (эксплуатационной) практики необходимо для успешного прохождения производственной (преддипломной) практики и написания выпускной квалификационной работы.

4. Структура и содержание практики

4.1 Очная форма обучения, 4 г., заочная форма обучения, 4г.8 мес. (всего 252 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. Изучение функциональных обязанностей должностного лица, в качестве которого проходит практика, и ознакомление с организацией рабочего места.	8	ПК-2	Л1.1-Л1.3
1.2	Рассмотрение штатной структуры организации. Анализ перспектив развития организации.	8	ПК-2	Л2.1-Л2.10
1.3	Изучение нормативно - правовых актов в области защиты информации; руководящих и методических	16	ПК-2 ПК-3	Л1.4

	документов уполномоченных федеральных органов исполнительной власти по защите информации; организационных мер по защите информации.			
1.4	Изучение принципов построения КС, стека сетевых протоколов операционных систем, стека протоколов сетевого оборудования и принципов функционирования сетевых протоколов, включающих криптографические алгоритмы.	16	ПК-2	Л1.4
1.5	Изучение видов политик управления доступом и информационными потоками в компьютерных сетях.	16	ПК-2	Л1.1
1.6	Выявление источников угроз информационной безопасности в компьютерных сетях и меры по их предотвращению.	16	ПК-2	
1.7	Изучение методов измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации.	16	ПК-2	Л1.1- Л1.4
1.8	Изучение типовых конфигураций программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях; принципов работы и правил эксплуатации эксплуатируемых программно-аппаратных средств защиты информации	16	ПК-2	Л1.1- Л1.4
1.9	Изучение архитектуры подсистемы защиты информации в операционных системах; принципов построения систем управления базами данных.	16	ПК-3	Л1.1- Л1.4
1.10	Изучение основных средств и методов анализа программных реализаций; принципов построения антивирусного программного обеспечения.	16	ПК-3	Л1.4
1.11	Изучение политики управления доступом и информационными потоками применительно к прикладному программному обеспечению.	16	ПК-3	Л1.1, Л1.4
1.12	Выявление: – источников угроз информационной безопасности программного обеспечения и меры по их предотвращению; – уязвимостей используемого программного обеспечения и методы их эксплуатации.	16	ПК-3	Л1.1- Л1.4
1.13	Изучение: – видов и форм функционирования вредоносного программного обеспечения; – характерных признаков наличия вредоносного программного обеспечения; – средств и методов обнаружения ранее неизвестного вредоносного программного обеспечения.	16	ПК-3	Л1.1- Л1.4
1.14	Изучение принципов функционирования программных средств криптографической защиты информации и порядка обеспечения безопасности информации при эксплуатации программного обеспечения.	14	ПК-3	Л1.4
1.15	Подведение итогов производственной (эксплуатационной) практики. Написание отчёта по производственной (эксплуатационной) практике и получение отзыва о проделанной работе.	8	ПК-3	Л1.1- Л1.3, Л3.1

Зачёт – 2 часа
Итого – 216 ч

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.)

– 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 14.07.2022) "О персональных данных"		Э1
Л2.2		Федеральный закон от 06.04.2011 N 63-ФЗ (ред. от 14.07.2022) "Об электронной подписи"		Э2
Л2.3		Федеральный закон от 07.07.2003 N 126-ФЗ (ред. от 30.12.2021) "О связи" (с изм. и доп., вступ. в силу с 01.05.2022)		Э3
Л2.4		Федеральный закон от 17.07.1999 N 176-ФЗ (ред. от 27.12.2019) "О почтовой связи"		Э4
Л2.5		Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 14.07.2022) "Об информации, информационных технологиях и о защите информации"		Э5
Л2.6		Закон РФ от 21.07.1993 N 5485-1 (ред. от 04.08.2022) "О государственной тайне"		Э6
Л2.7		Указ Президента РФ от 17.03.2008 N 351 (ред. от 22.05.2015) "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена"		Э7
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	Енгибарян И.А.	Методические указания по проведению Производственной (эксплуатационной) практики для студентов по направлению подготовки 10.03.01	РнД: СКФ МТУСИ, 2022	Э11

7.2. Электронные образовательные ресурсы

Э1	http://www.consultant.ru/cons/cgi/online.cgi?from=178749
Э2	http://www.consultant.ru/cons/cgi/online.cgi?from=191956
Э3	http://www.consultant.ru/cons/cgi/online.cgi?from=201564
Э4	http://www.consultant.ru/cons/cgi/online.cgi?from=201192
Э5	http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=422054&rnd=GxYjg#9dKVe
Э6	http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=423720&rnd=GxYjg#FItVeG

Э7	https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=180102&dst=
Э8	https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702-prikaz-fstek-rossii-ot-11-fevralya-2013
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 (эксплуатационная) 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