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 (преддипломная) практика
Б2.В.03(Пд)
рабочая программа

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 (6 недель)	216/8		
Контактная работа, в том числе (по семестрам, курсам):				
Самостоятельная работа		216/8		
Число зачетов с разбивкой по семестрам (курсам)		1/8		
Способы и формы проведения производственной практики				
Способ проведения	Стационарная Выездная		Стационарная Выездная	
Форма проведения	Дискретная		Дискретная	

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

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

Рабочая программа
Производственная (преддипломная) практика

Разработана в соответствии с ФГОС ВО
направления подготовки 11.03.02 ИНФОКОММУНИКАЦИОННЫЕ направления подготовки 10.03.01 «Информационная безопасность», утвержденным приказом Министерства образования и науки Российской Федерации от 17 ноября 2020г. N 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 «29» 08 20 22 г. № 1

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 ИТСС

Протокол от _____ 20___ г. № ___

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 ИТСС

Протокол от _____ 20___ г. № ___

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 ИТСС

Протокол от _____ 20___ г. № ___

Зав. кафедрой _____ В.И. Юхнов

Утверждаю
Зам. директора по УВР
_____ _____ 20___ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры ИТСС

Протокол от _____ 20___ г. № ___

Зав. кафедрой _____ В.И. Юхнов

1. Цели производственной практики

Целями производственной 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 **эксплуатационной** деятельностью.

Результатом освоения дисциплины являются сформированные у выпускника следующие компетенции:

ПК-1 Администрирование подсистем защиты информации в операционных системах
Знать (Необходимые знания):
- архитектуру и принципы построения операционных систем; - программные интерфейсы операционных систем; - виды политик управления доступом и информационными потоками применительно к операционным системам; - архитектуру подсистем защиты информации в операционных системах; - принципы функционирования средств защиты информации в операционных системах, в том числе использующих криптографические алгоритмы; - состав типовых конфигураций программно-аппаратных средств защиты информации; - требования по составу и характеристикам подсистем защиты информации применительно к операционным системам; - порядок реализации методов и средств антивирусной защиты в операционных системах; - программно-аппаратные средства и методы защиты информации в операционных системах; - принципы работы и правила эксплуатации программно-аппаратных средств защиты информации; - 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 (Необходимые умения):
- формулировать политики безопасности операционных систем; - настраивать политики безопасности операционных систем; - оценивать угрозы безопасности информации операционных систем; - противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации операционных систем; - выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах; - настраивать антивирусные средства защиты информации в операционных системах; - устанавливать обновления программного обеспечения и средств антивирусной защиты; - проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах; - производить анализ эффективности программно-аппаратных средств защиты информации в операционных системах; - оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах.

Владеть (Трудовые действия):

- определением состава применяемых программно-аппаратных средств защиты информации в операционных системах;
- разработкой порядка применения программно-аппаратных средств защиты информации в операционных системах;
- формированием шаблонов установки программно-аппаратных средств защиты информации в операционных системах;
- установкой программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации;
- конфигурированием программно-аппаратных средств защиты информации в операционных системах;
- контролем корректности функционирования программно-аппаратных средств защиты информации в операционных системах;
- управлением антивирусной защитой операционных систем в соответствии с действующими требованиями.

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 практики в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Производственная (преддипломная) практика является логическим продолжением изучения дисциплин Б1.О.33 Программно-аппаратные средства защиты информации Б1.О.35 Криптографические протоколы Б1.О.37 Комплексное обеспечение защиты информации Б1.О.40 Администрирование средств защиты информации в компьютерных системах и сетях Б2.В.02(П) Производственная (эксплуатационная) практика
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Прохождение производственной (преддипломной) практики необходимо для успешного написания выпускной квалификационной работы.

4. Структура и содержание практики

4.1 Очная форма обучения, 4 г., (всего 216 часов)

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.	4	ПК-1, ПК-2, ПК-3	Л1.1-Л1.3
1.2	Библиографический поиск	22	ПК-1, ПК-2, ПК-3	Л2.1-Л2.10
1.3	Изучение нормативно-технической документации	32	ПК-1, ПК-2, ПК-3	Л1.4
1.4	Участие в измерениях или отладке оборудования и программного обеспечения систем и устройств программной защиты информации	50	ПК-1, ПК-2, ПК-3	Л1.4
1.5	Изучение требований по размещению криптографического оборудования	20	ПК-1, ПК-2, ПК-3	Л1.1-Л1.4
1.6	Рассмотрение вопросов применения дополнительного оборудования для информационной защиты компьютерной сети предприятия	20	ПК-1, ПК-2, ПК-3	Л1.1-Л1.4
1.7	Подготовка технической документации и необходимых заявок на ремонт или замену оборудования, а также обновление или замену программного обеспечения.	26	ПК-1, ПК-2, ПК-3	Л1.1-Л1.4
1.8	Ознакомление со структурой и содержанием типовых ВКР бакалавра.	20	ПК-1, ПК-2, ПК-3	Л1.4
1.9	Обобщение результатов работы. Написание отчёта по производственной (преддипломной) практике и получение отзыва о работе во время практики.	20	ПК-1, ПК-2, ПК-3	Л1.1-Л1.3, Л3.1
Зачёт – 2 часа				
Итого – 216 часов				

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.	Производитель 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	Юхнов В.И.	Методические указания по проведению Производственной (преддипломной) 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?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 практика организуется на предприятиях или в организациях, в которых имеются компьютерные сети. Возможно проведение практики на предприятиях, обладающих собственной развитой корпоративной сетью, на должностях, связанных с её эксплуатацией.

В перечисленных организациях должен находиться ряд оборудования, 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