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
_____ Н.А. Андреева
«29» 04 2024 г.

Производственная (технологическая) практика Б2.В.02(П)

рабочая программа дисциплины

Кафедра: **Информационной безопасности**
Направление подготовки: **10.03.01 Информационная безопасность**
Профиль: **Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)**
Формы обучения: **очная**

Распределение часов дисциплины по семестрам (для очной формы обучения (ОФО))

Объем и структура производственной практики по семестрам		
Вид учебной работы	ОФО	
	ЗЕ	часов
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	3 (2 недель)	108/6
Контактная работа, в том числе (по семестрам, курсам):		2/6
Самостоятельная работа		106/6
Число зачетов с оценкой с разбивкой по семестрам (курсам)		1/6
Способы и формы проведения производственной практики		
Способ проведения	Стационарная Выездная	
Форма проведения	Дискретная	

Программу составил:
заведующий кафедрой ИБ, к.т.н., доцент Маршаков Д.В.

Рецензенты:
ведущий научный сотрудник «Ростовский-на-Дону НИИ радиосвязи»,
д.т.н., доцент Погорелов В.А.

Рабочая программа дисциплины
«Производственная (технологическая) 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 2020 г. N 1427.

Составлена на основании учебного плана
направления 10.03.01 «Информационная безопасность», профиля «Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)», одобренного Учёным советом СКФ МТУСИ, протокол № 9 от 22.04.2024, и утвержденного директором СКФ МТУСИ 22.04.2024 г.

Рассмотрена и одобрена на заседании кафедры
«Информационная безопасность»

Протокол от «24» апреля 2024 г. № 9

Зав. кафедрой _____ Д.В. Маршаков

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

Утверждаю
Зам. директора по УВР _____
-__ _____ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры
"Информационная безопасность"

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

"Информационная безопасность"

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
"Информационная безопасность"

Протокол от _ _____ 20__ г. № _
Зав. кафедрой _____

---

1. Цели изучения дисциплины

Целями изучения дисциплины ***"Производственная (технологическая) практика"*** является закрепление и углубление теоретической подготовки по направлению подготовки 10.03.01 Информационная безопасность, получение обучающимися практических навыков и компетенций по видам профессиональной деятельности, приобретение практических навыков и компетенций в сфере профессиональной деятельности и их применение при решении производственных задач.

Задачи производственной практики:

- изучение теоретических и экспериментальных методов получения, обработки и хранения научной информации с привлечением современных информационных технологий; - изучение опыта проведения конкретных научных исследований в организации и лабораториях кафедры университета,
- развитие навыков сбора, обработки, анализ и систематизации научно-технической информации по теме исследования;
- выбор методик и средств решения поставленных задач;
- изучение форм и порядка составления отчетной научно-технической документации и внедрения результатов научных исследований;
- формирование навыков ведения научных исследований, как целостного процесса, в том числе навыков анализа конкретной проблемной ситуации, формулировки проблемы и выдвижения гипотезы, разработки плана эксперимента, проведения эксперимента, обработки результатов, формулировки выводов и представления итогов проделанной работы в виде научных отчетов, рефератов или статей;
- разработка плана и программы проведения научных исследований и технических разработок по выбранной теме исследования.

Вид практики: производственная
Тип практики: технологическая

2. Планируемые результаты обучения

Изучение дисциплины направлено на формирование у выпускника способности решать профессиональные задачи в соответствии с ***организационно-управленческой и эксплуатационной деятельностью.***

Результатом освоения дисциплины являются сформированные у выпускника следующие компетенции:

Компетенции выпускника, формируемые в результате освоения дисциплины (в части, обеспечиваемой дисциплиной)
ПК-2. Способен участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты
Знать:
- виды политик безопасности компьютерных систем и сетей; - модели безопасности компьютерных систем; - организационные меры по обеспечению информационной безопасности объекта защиты.
Уметь:
- анализировать объект защиты информации с целью определения необходимого уровня защищенности и доверия; - формулировать задания по обеспечению информационной безопасности объекта защиты.
Владеть:

- навыками формирования политики безопасности компьютерных систем и сетей; - навыками разработки профилей защиты компьютерных систем.
ПК-4. Способен организовывать безопасную эксплуатацию и выполнять администрирование общего и специального программного обеспечения
Знать:
- состав типовых конфигураций программно-аппаратных средств защиты информации и режимов их функционирования в компьютерных системах и сетях; - источники угроз информационной безопасности в компьютерных системах и сетях и меры по их предотвращению.
Уметь:
- обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных системах и сетях; - выбирать режимы работы программно-аппаратных средств защиты информации в компьютерных системах и сетях.
Владеть:
- навыками конфигурирования и контроля корректности настройки программно-аппаратных средств защиты информации в компьютерных системах и сетях; - навыками мониторинга функционирования программно-аппаратных средств защиты информации в компьютерных системах и сетях.

3. Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Б1.О.30 Программно-аппаратные средства защиты информации
2	Б1.В.03 Защита информации от вредоносного программного обеспечения
3	Б1.О.32 Основы управления информационной безопасностью
4	Б1.О.29 Методы и средства криптографической защиты информации
5	Б1.В.04 Разработка безопасного программного обеспечения (Проектирование защищенных информационных систем)
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Б1.О.36.03 Безопасность компьютерных сетей
2	Б1.О.36.04 Безопасность систем баз данных
3	Б1.О.31 Защита информации от утечки по техническим каналам

Рабочая программа дисциплины для инвалидов и лиц с ограниченными возможностями здоровья разрабатывается индивидуально с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 108 часов, 2 часа контактной работы, 106 часов самостоятельной работы)

Код зан.	Тема и краткое содержание работы	Кол. часов	Компетенции	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.	4	ПК-2	Л1.1-Л1.3
1.2	Рассмотрение штатной структуры организации. Анализ	4	ПК-2	Л2.1-

	перспектив развития организации.			Л2.10
1.3	Изучение нормативно - правовых актов в области защиты информации; руководящих и методических документов уполномоченных федеральных органов исполнительной власти по защите информации; организационных мер по защите информации.	8	ПК-2 ПК-4	Л1.4
1.4	Изучение принципов построения КС, стека сетевых протоколов операционных систем, стека протоколов сетевого оборудования и принципов функционирования сетевых протоколов, включающих криптографические алгоритмы.	8	ПК-2	Л1.4
1.5	Изучение видов политик управления доступом и информационными потоками в компьютерных сетях.	8	ПК-4	Л1.1
1.6	Выявление источников угроз информационной безопасности в компьютерных сетях и меры по их предотвращению.	8	ПК-4	
1.7	Изучение методов измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации.	8	ПК-4	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	8	ПК-4	Л1.1- Л1.4
1.9	Изучение архитектуры подсистемы защиты информации в операционных системах; принципов построения систем управления базами данных.	8	ПК-2	Л1.1- Л1.4
1.10	Изучение основных средств и методов анализа программных реализаций; принципов построения антивирусного программного обеспечения.	8	ПК-2	Л1.4
1.11	Изучение политики управления доступом и информационными потоками применительно к прикладному программному обеспечению.	8	ПК-2	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.	8	ПК-2	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.	8	ПК-2	Л1.1- Л1.4
1.14	Изучение принципов функционирования программных средств криптографической защиты информации и порядка обеспечения безопасности информации при эксплуатации программного обеспечения.	6	ПК-2	Л1.4
1.15	Подведение итогов производственной (технологической) практики. Написание отчёта по производственной (технологической) практике и получение отзыва о про-	4	ПК-2	Л1.1- Л1.3, Л3.1

	деланной работе.			
Зачёт с оценкой – 2 часа				
Итого – 108 ч				

5. 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		Э1

		(ред. от 14.07.2022) "О персональных данных"		
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#9dK

	Ve
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	Linux (свободное ПО)
П.2	LibreOffice (свободное ПО)
П.3	Kaspersky Endpoint Security (лицензия)

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.

7. Методические рекомендации для обучающихся по самостоятельной работе

Перед прохождением практики обучающийся должен изучить программу, представленную учебно-методическую документацию по практике и обратиться к соответствующим нормативным материалам, литературе с тем, чтобы быть подготовленным к выполнению поручений, данных руководителем практики, к решению задач практики, конкретных практических вопросов.

В случае прохождения практики на предприятиях обучающиеся при необходимости должны подготовить необходимые документы (получить медицинскую справку по форме, требуемой предприятием-базой практики, подготовить фотографии и паспортные данные (ксерокопии разворотов с фотографией и регистрацией места жительства для оформления пропусков на предприятии и т.д.).

В рамках самостоятельной работы обучающимся рекомендуется просмотреть конспекты лекций, учебники и другие учебные издания.

Контроль качества самостоятельной работы обучающихся производится при защите отчета по практике. При прохождении практики обучающиеся обязаны: своевременно прибыть на место прохождения практики, иметь при себе все необходимые документы: индивидуальное задание, план (график) практики; подчиняться действующим правилам внутреннего трудового распорядка организации - места прохождения практики; изучить и строго соблюдать правила охраны труда, техники безопасности, пожарной безопасности; выполнять задания, предусмотренные программой практики; быть вежливым, внимательным в общении с работниками; вести записи о проделанной работе, чтобы в дальнейшем в отчете описать содержание проделанной работы; в установленный срок отчитаться о

прохождении практики руководителю практики от университета, подготовить и сдать отчет и другие документы по практике на кафедру.

При подготовке к практике и во время прохождения практики рекомендуется по возникшим вопросам обращаться к учебной литературе, методическим материалам. При возникновении затруднений в процессе практики обучающийся может обратиться к руководителю практики от университета либо от организации-базы практики и получить необходимые разъяснения.

.

Источники, рекомендуемые для углубленного изучения учебного материала

1. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие. – М.: ДМК Пресс, 2011. – 416 с.;
2. Бирюков А.А. Информационная безопасность: защита и нападение. 2-е изд., перераб. и доп. – М.: ДМК Пресс, 2017. – 434 с.
3. Маршаков, Д. В. Программно-аппаратные средства защиты информации: учебное пособие / Д. В. Маршаков, Д. В. Фатхи. — Ростов-на-Дону: Донской ГТУ, 2021. — 228 с.
4. Воронов В.А., Тихонов В.А. Концептуальные основы создания и применения системы защиты объектов. – М.: Горячая линия - Телеком, 2013.
5. Хорев П.Б. Программно-аппаратная защита информации: учебное пособие. 3-е изд., испр. и доп. – Москва: ИНФРА-М, 2022. – 327 с.
6. Ерохин С.Д., Петухов А.Н., Пилюгин П.Л. Управление безопасностью критических информационных инфраструктур. – М.: Горячая линия – Телеком, 2021.
7. Климентьев, К. Е. Введение в защиту компьютерной информации: учебное пособие / К. Е. Климентьев. — Самара: Самарский университет, 2020. — 183 с.
8. Краковский, Ю. М. Методы защиты информации: учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург: Лань, 2021. — 236 с..
9. Никифоров, С. Н. Методы защиты информации. Пароли, скрытие, шифрование: учеб-ное пособие для вузов / С. Н. Никифоров. — 4-е изд., стер. — Санкт-Петербург: Лань, 2022. — 124 с.
10. Язов Ю.К., Соловьев С.В. Организация защиты информации в информационных системах от несанкционированного доступа: монография / Ю.К. Язов, С.В. Соловьев. – Воронеж: Кварта, 2018. – 588 с.
11. Профильные журналы «Электросвязь», «T-Comm: Телекоммуникации и транспорт» и другие.

Использование Интернет-ресурсов

1. Электронный ресурс https://www.securitylab.ru/
2. Электронный ресурс https://securelist.ru/
3. Электронный ресурс https://www.kaspersky.ru/
4. Электронный ресурс https://encyclopedia.kaspersky.ru/
5. Электронный ресурс https://www.drweb.ru/
6. Электронный ресурс http://infoprotect.net/category/news
7. Электронный ресурс https://www.it-world.ru/it-news/security/
8. Электронный ресурс https://threatpost.ru/
9. Электронный ресурс https://www.anti-malware.ru/

Рекомендации по подготовке к рубежным аттестациям

Система оценки качества прохождения практики предусматривает следующие виды контроля: текущий контроль; промежуточная аттестация.

Текущий контроль осуществляется руководителем от университета и проводится в форме предварительной проверки материалов по практике.

Промежуточная аттестация проводится в форме зачета с оценкой в виде защиты отчетов по практике. При проведении промежуточной аттестации обучающегося учитываются результаты текущего контроля.

В соответствии с целью практики в зависимости от места ее прохождения руководителем практики от кафедры формируются задания на практику индивидуально каждому обучающемуся.

Отчет по практике должен быть выполнен в объеме 10-15 страниц и включать в себя разделы, полностью отражающие содержание пройденной практики.

Аттестация по итогам практики проводится на основании оформленного в соответствии с установленными требованиями письменного отчета и отзыва руководителя от практики. Отчет по практике должен содержать: титульный лист, индивидуальное задание, рабочий график (план) проведения практики, оглавление, введение, основная часть, заключение, список литературы, приложения (при необходимости). Подготовленный отчет подписывается студентом и руководителем практики от кафедры.

Промежуточную аттестацию в форме зачета с оценкой по практике проводит руководитель практики в месячный срок после начала занятий в 7-м семестре при предоставлении обучающимся оформленных дневника, отчета по практике, аттестационного листа и характеристики. Результаты промежуточной аттестации проставляются в ведомости и зачетной книжке обучающегося..

Дополнения и изменения в Рабочей программе