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.

Введение в профессию Б1.В.08

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))

Вид учебной работы	ОФО	
	ЗЕ	часов
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	4	144/1 сем
Контактная работа, в том числе (по семестрам, курсам):		54/1 сем
Лекции		36/1 сем
Лабораторных работ		
Практических занятий		18/1 сем
Семинаров		
Самостоятельная работа		90/1 сем
Контроль		
Число контрольных работ (по курсам)		
Число КР (по семестрам, курсам)		
Число КП (по семестрам, курсам)		
Число зачетов с разбивкой по семестрам (курсам)		1/1 сем
Число экзаменов с разбивкой по семестрам (курсам)		

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
«Введение в профессию»

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 ***"Введение в профессию"*** являются формирование у обучаемых знаний в области основ информационной безопасности и навыков практического обеспечения защиты информации и безопасного использования программных и аппаратных средств в компьютерных системах.

2. Планируемые результаты обучения

Изучение дисциплины направлено на формирование у выпускника способности решать профессиональные задачи в соответствии с ***проектно-технологической деятельностью.***

Результатом освоения дисциплины являются сформированные у выпускника следующие компетенции:

Компетенции выпускника, формируемые в результате освоения дисциплины (в части, обеспечиваемой дисциплиной)
УК-6: способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни
Знать:
- основные приемы эффективного управления собственным временем; основные методики самоконтроля, саморазвития и самообразования на протяжении всей жизни. - направления обеспечения информационной безопасности
Уметь:
- эффективно планировать и контролировать собственное время; использовать методы саморегуляции, саморазвития и самообучения
Владеть:
- методами управления собственным временем; технологиями приобретения, использования и обновления социокультурных и профессиональных знаний, умений и навыков; методиками саморазвития и самообразования в течение всей жизни

3. Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
Изучение данной дисциплины базируется на общих знаниях и коммуникативных компетенциях, полученных на предыдущих уровнях образования	
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Б1.О.27 Основы информационной безопасности

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 144 часов, 54 аудиторных часов, 90 часов самостоятельной работы)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
Курс 1, Семестр 1					
Модуль 1: Информация и организационное обеспечение её безопасности					
1.1	Лекция 1. Информация и информационная безопасность Определение и классификация. Информация и доку-	Лек.	2	УК-6	Л1.1 Л1.2

	ментооборот. Информация как объект защиты				
1.2	Лекция 2. Обработка и передача информации в компьютерных системах и сетях. Структурная информационной (автоматизированной системы). Машинное представление информации.	Лек.	2	УК-6	Л1.1 Л1.2
1.3	Лекция 3. Общие вопросы информационной безопасности и защиты данных. Исторические аспекты ИБ. Виды организационного управления. Угрозы ИБ и их источники	Лек.	4	УК-6	Л1.1
1.4	Лекция 4. Правовое обеспечение информационной безопасности. Доктрина ИБ РФ. Введение в проблематику обеспечения безопасности компьютерных систем	Лек.	4	УК-6	Л1.1 Л1.2
1.5	Лекция 5. Каналы утечки конфиденциальных данных. Виды каналов утечки. Классификация технических каналов утечки конфиденциальной информации	Лек.	4	УК-6	Л1.1
1.6	Практическое занятие №1 Инструментарий этичного хакинга и пентестинга	Пр.	2	УК-6	Л1.1
1.7	Практическое занятие №2 Криптография и программы-вымогатели	Пр.	2	УК-6	Л1.1
1.8	Практическое занятие №3 Протокол TLS и алгоритм Диффи — Хеллмана	Пр.	2	УК-6	Л1.1
1.9	Практическое занятие №4 Фишинг и сбор информации	Пр.	2	УК-6	Л1.1
1.10	Кибератаки предприятий в XXI веке. Российские и зарубежные стартапы в области ИБ. Форензика как наука о расследовании киберпреступлений. Вредоносные приложения для Android и iOS (обзор, конкретные примеры, последствия). Технология SIEM. История развития технологии распознавания образов. Информационная война и ее влияние на национальную безопасность государства. Соревнования по информационной безопасности по стандартам CTF. Современные алгоритмы шифрования. Защита персональных данных: регулировании в России и США.	СРС	50	УК-6	Л1.1 Л2.1
Модуль 2: Основы информационной безопасности					
2.1	Лекция №6. Основы безопасности вычислительных сетевых технологий. Компьютерные сети. Эталонная модель OSI. Перехват трафика.	Лек.	4	УК-6	Л1.1 Л1.2
2.2	Лекция №7. Основы безопасности баз данных Архитектура системы управления базами данных (СУБД). Угрозы информационной безопасности баз данных.	Лек.	4	УК-6	Л1.2 Л2.3
2.3	Лекция №8. Основы безопасности операционных систем Архитектура операционных систем. Угрозы безопасности операционных систем.	Лек.	4	УК-6	Л1.1 Л1.2

2.4	Лекция №9. Основы защиты информации от НСД. Общая характеристика и классификация мер и средств защиты информации от несанкционированного доступа (НСД). Требования к мерам защиты информации от НСД, реализуемым в автоматизированной (информационной) системе	Лек.	4	УК-6	Л1.1 Л2.1
2.5	Лекция №10. Социальная инженерия Феномен. Кибермошенничество. Фишинг. Сбор информации.	Лек.	4	УК-6	Л1.1 Л1.2 Л2.2
2.6	Практическое занятие №5 Перехват и анализ трафика	Пр.	2	УК-6	Л1.1 Л2.1 Л2.2
2.7	Практическое занятие №6 Эксплуатация уязвимостей	Пр.	4	УК-6	Л1.1
2.8	Практическое занятие №7 Настройка разграничений доступа штатными средствами ОС	Пр.	2	УК-6	Л1.1 Л1.2
2.9	Практическое занятие №8 Парольная защита информации	Пр.	2	УК-6	Л1.1 Л1.2
2.10	Виртуальные частные сети. Служба управления сетью. Иерархия средств защиты от информационных угроз. Принципы защиты информационной системы. Шифрование. Метод Диффи-Хелмана. Хеш-функции. Атаки на транспортную инфраструктуру сети. Облачные сервисы и их безопасность.	СРС	40	УК-6	Л1.1 Л2.1
	Итого		144		

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Рекомендуемая литература				
5.1.1. Основная литература				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**
Л1.1	Олифер В.Г., Олифер Н.А.	Компьютерные сети. Принципы, технологии, протоколы.	СПб.: Питер, 2016. 992 с.	5
Л1.2	Малюк А.А., Горбатов В.С., Королев В.И., Фомичев В.М., Дураковский А.П., Кондратьева Т.А.	Введение в информационную безопасность	М.: Гор. линия-Телеком, 2018. – 288 с.	Э1
5.1.2. Дополнительная литература				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**
Л2.1	Малюк А.А.	Защита информации в информационном обществе	М.: Гор. линия-Телеком, 2015. – 230 с.	Э2
Л2.2	Е. Б. Белов,	Основы информационной безопасно-	М.: Гор. линия-	Э3

	В.П. Лось, Р. В. Мещеряков, Д. А. Шелупанов	сти	Телеком, 2011. - 558	
Л2.3	Шаньгин В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2019. — 702 с. — ISBN 978-5-4488-0070-2	Э4

5.2. Электронные образовательные ресурсы	
Э1	https://znanium.com/catalog/document?id=42509
Э2	https://znanium.com/catalog/document?id=257570
Э3	https://znanium.com/catalog/document?id=233208
Э4	https://www.iprbookshop.ru/87995.html
5.3. Программное обеспечение	
П.1	Linux
П.2	LibreOffice
П.3	Python 3
П.4	VM Kali Linux
П.5	VM pfSense
П.6	VM Ubuntu Linux
П.7	VM Metasploitable

6. Материально-техническое обеспечение дисциплины

6.1 МТО лекционных занятий	
1	Лекционная аудитория, оборудованная интерактивной доской, проектором
6.2 МТО лабораторных работ и практических занятий	
1	Компьютерные аудитории с возможностью выхода в локальную сеть Филиала и Интернет
6.3 МТО рубежных контролей, экзамена	
1	Компьютерные аудитории с возможностью выхода в локальную сеть Филиала и Интернет

7. Методические рекомендации для обучающихся по самостоятельной работе

Указания по подготовке к различным видам занятий

Подготовка к лекционным занятиям осуществляется систематически и сводится к повторению изученного материала и отработке тем, вынесенных на самостоятельную работу. При этом должен быть доработан конспект лекций, а также получены ответы на контрольные вопросы, которые, как правило, приводятся в конце каждого раздела учебных пособий. Особое внимание необходимо уделить пониманию изучаемого материала. Зафиксировать вопросы, которые следует задать преподавателю.

Подготовка к лабораторным и практическим занятиям должна проводиться в объеме тех указаний, которые приводятся в каждом методическом пособии для проведения соответствующего занятия. Тема очередного занятия объявляется преподавателем накануне.

После повторения лекционного материала необходимо ознакомиться с предлагаемыми практическими заданиями, уяснить их суть, продумать порядок их выполнения, уточнить достаточность своих знаний для выполнения задания. Целесообразно выполнить возможные заготовки из состава отчета, который предстоит оформить на занятии. Это позволит выполнить и защитить работу в период плановых часов. Перед проведением каждого занятия должно быть полное представление о сути и порядке выполнения предстоящей работы.

Существенное значение имеет самостоятельная работа студента.

Темы для самостоятельного изучения для различных форм обучения, информационные источники и рекомендуемое время указаны в Разделе 4 настоящей Рабочей программы.

Самостоятельная работа студентов по дисциплине проводится в течение всего семестра и складывается из нескольких составляющих.

Подготовка к плановым аудиторным занятиям. В начале семестра студентов знакомят с календарным планом проведения всех видов учебных занятий. Чтобы студенты могли проверить качество своей подготовки к занятиям, в учебных пособиях и методических указаниях к лабораторным работам имеются вопросы для проверки уровня знаний перед выполнением работы и контрольные вопросы, позволяющие студенту оценить качество полученных результатов после выполнения работы. Предлагаемые студентам учебные пособия кроме контрольных вопросов содержат примеры с решениями и упражнения по основным темам.

Изучение технической литературы. Студенты самостоятельно изучают рекомендованную преподавателем техническую литературу.

Дополнительные самостоятельные исследования в лаборатории. Студенты, желающие получить более глубокие знания, имеют возможность выполнить дополнительные самостоятельные исследования в лаборатории. С этой целью в плановых лабораторных работах предусмотрены возможности для дополнительных исследований. Перечень разделов программы, предлагаемых для самостоятельных исследований, доводится до сведения студентов в начале семестра.

Самостоятельная работа на ПЭВМ. Для повышения эффективности самостоятельной работы студентам во второй половине дня предоставляется возможность выполнить в лаборатории самостоятельные исследования с использованием программно-аппаратного комплекса, состоящего из виртуальных электронных приборов, отображаемых на экране ПЭВМ, и моделирующих программ. Исследуемые схемы могут собираться из реальных компонентов на лабораторном стенде или виртуальных компонентов, хранящихся в библиотеке ПЭВМ.

Источники, рекомендуемые для углубленного изучения учебного материала

1. Конституция Российской Федерации.
2. Малюк А.А., Горбатов В.С., Королев В.И., Фомичев В.М., Дураковский А.П., Кондратьева Т.А. Введение в информационную безопасность. – М.: Горячая линия-Телеком, 2018.
3. Медведев В.А. Информационная безопасность. Введение в специальность.–М.: КноРус, 2021, -144 с.
4. Грэм Д.Г. Этичный хакинг. Практическое руководство по взлому. — СПб.: Питер, 2022. — 384 с.
5. Бегаев А.Н., Бегаев С.Н., Федотов В.А. Тестирование на проникновение: Учебное пособие. – СПб: Университет ИТМО, 2018. – 43 с.
6. Бирюков А.А. Информационная безопасность: защита и нападение. 2-е изд., перераб. и доп. – М.: ДМК Пресс, 2017. – 434 с.
7. Бондарев В.В. Анализ защищенности и мониторинг компьютерных сетей. Методы и средства: учебное пособие. – М.: Издательство МГТУ им. Н.Э. Баумана, 2017. – 225 с

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

Подготовка к сдаче модуля сводится защите на дату проведения последнего занятия в рамках модуля всех практических и лабораторных занятий, а также к подготовке к ответам по тестовым заданиям.

Объем вопросов по каждому лабораторному и практическому занятию отражен в методических указаниях по проведению соответствующего занятия. Кроме того студент должен быть готов к пояснениям по сути практических приемов работы и доказыванию обоснованности принятых решений. Если работа не выполнена или не защищена своевременно, то это следует сделать в часы самоподготовки и консультаций до даты последнего занятия в рамках сдаваемого модуля.

Подготовка к выполнению теста обеспечивается изучением и повторением того материала, который изучался на лекционных занятиях и входе лабораторных и практических занятий. Материал повторяется по конспектам и учебным пособиям, указанным в списке литературы и методических указаниях.

Подготовка к зачету осуществляется на протяжении всего времени изучения дисциплины.

Для более конкретной, целенаправленной и качественной подготовки к зачету необходимо перед началом изучения дисциплины познакомиться с содержанием рабочей программы. Уяснить логику и последовательность изучения материала, уточнить конкретные конечные результаты, которые должны быть достигнуты в итоге изучения конкретных тем и занятий. Познакомиться с перечнем вопросов и заданий, выносимых на экзамен.

В ходе каждого занятия необходимо изучить все учебные вопросы и выполнить практические задания. Для оперативного оценивания уровня достижения учебных целей следует ответить на контрольные вопросы, которые имеются в руководстве для каждого практического и лабораторного занятия. В случае выявленных затруднений следует провести дополнительное изучение материала в часы самостоятельной работы или в период консультаций с преподавателем. Все учебные материалы должны быть отражены в конспекте, он должен дополняться и уточняться по мере отработки и уточнения учебных вопросов. Само ведение конспекта концентрирует внимание, упорядочивает знания, стимулирует активность в усвоении. К моменту выхода на непосредственную подготовку к зачету в конспекте не должно остаться непонятных вопросов.

В силу ограниченного времени, отводимого на непосредственную подготовку к зачету, целесообразно материал повторять в основном по отработанному конспекту. Это экономит время и дает возможность работать по уже знакомым записям, что улучшает запоминание материала. Остается спланировать работу в соответствии с имеющимся временем и жестко придерживаться намеченного плана. В период обязательных плановых предэкзаменационных консультаций необходимо уточнить организационные вопросы проведения экзамена и при необходимости - сложные вопросы по существу материала.

Дополнения и изменения в Рабочей программе