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.

Введение в профессию Б1.В.01
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):	3	108/1сем		
Контактная работа, в том числе (по семестрам, курсам):		54/1сем		
Лекции		22/1сем		
Лабораторных работ				
Практических занятий		32/1сем		
Семинаров				
Самостоятельная работа		54/1сем		
Контроль				
Число контрольных работ (по курсам)				
Число КР (по семестрам, курсам)				
Число КП (по семестрам, курсам)				
Число зачетов с разбивкой по семестрам (курсам)		1/1сем		
Число экзаменов с разбивкой по семестрам (курсам)				

Программу составил:
Доцент кафедры ИТСС, к.т.н., доцент Борисов Б.П.

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

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 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 «29» 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

Целью преподавания дисциплины «Введение в профессию» является формирование у обучаемых знаний в области основ информационной безопасности и навыков практического обеспечения защиты информации и безопасного использования программных и аппаратных средств в сетях и информационных системах.

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)
ОПК-1: Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства
Знать:
- понятия информации и информационной безопасности, место и роль информационной безопасности в системе национальной безопасности Российской Федерации; - направления обеспечения информационной безопасности; - классификацию методов криптографического преобразования информации; - структуру и принципы функционирования современных вычислительных систем; - основные способы защиты от потери информации и нарушений работоспособности сетей и систем.
Уметь:
- классифицировать и оценивать угрозы информационной безопасности; - проводить работы по сокрытию информации, проведению резервного копирования, восстановления информации; - использовать механизмы идентификации и аутентификации; - использовать антивирусные средства защиты; - производить резервное копирование.
Владеть:
- основными понятиями, связанными с обеспечением информационно-психологической безопасности личности, общества и государства; информационного противоборства, информационной войны и формами их проявления в современном мире; - навыками работы по основам защиты информации с использованием программно-аппаратных комплексов.

3. Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Дисциплина «Введение в профессию Б1.В.01» базируется на знаниях, приобретенных из дисциплин: Б1.О.03 «Информатика», Б1.О.06 «Физика», Б1.О.07 «Иностранный язык».
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Дисциплина является базовой для успешного освоения дисциплин: Б1.О.25 «Основы информационной безопасности»

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 108 часов, 60 аудиторных часов, 48 часов самостоятельной работы)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
Курс 1, Семестр 1					
Модуль 1. Основы сетей передачи данных (26+26) часов					
1.1	Лекция 1 Эволюция компьютерных сетей 1. Системы пакетной обработки 2. Многотерминальные системы – прообраз сети 3. Первые компьютерные сети 4. Конвергенция сетей	Л1.	2	ОПК-1	Л1.1 Л1.2
1.2	Лекция 2 Общие принципы построения сетей 1. Простейшая сеть из двух компьютеров 2. Сетевое программное обеспечение 3. Физическая передача данных по линиям связи 4. Связь нескольких компьютеров	Л2.	2	ОПК-1	Л1.1 Л1.2
1.3	Практическое занятие №1 Организация простейшей сети 1. Анализ интерфейсов ПК 2. Установление сетевого соединения 3. Передача различных видов трафика между компьютерами	Пз №1	4	ОПК-1	Л1.1
1.4	Лекция 3 Коммутация каналов и пакетов 1. Коммутация каналов 2. Коммутация пакетов 3. Ethernet – стандартная технология с коммутацией пакетов	Л3.	2	ОПК-1	Л1.1 Л1.2
1.5	Практическое занятие №2 Обобщенная задача коммутации 1. Определение информационных потоков 2. Маршрутизация потоков 3. Продвижение потоков 4. Мультиплексирование и демультиплексирование потоков	Пз №2	4	ОПК-1	Л1.1
1.6	Лекция 4 Архитектура, стандартизация и классификация сетей 1. Декомпозиция задачи сетевого взаимодействия 2. Модель OSI 3. Стандартизация сетей 4. Информационные и транспортные услуги	Л4.	2	ОПК-1	Л1.1
1.7	Практическое занятие №3 Взаимодействие открытых систем 1. Понятие открытой системы 2. Стандартные стеки коммуникационных протоколов 3. Обмен сообщениями	Пз №3	4	ОПК-1	Л1.1

1.8	Лекция 5 Сетевые характеристики 1. Типы характеристик 2. Производительность и надежность сети 3. Характеристики сети поставщика услуг	Л5.	2	ОПК-1	Л1.1
1.9	Практическое занятие №4 Передача пакетов 1. Распределение протоколов по элементам сети 2. Количественные характеристики и требования 3. Передача пакетов и статистические оценки характеристик сети	Пз №4	4	ОПК-1	Л1.1
1.10	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). Коммутируемые сети Ethernet. Кодирование и мультиплексирование данных. Беспроводная передача данных. Технологии локальных сетей на разделяемой среде.	СР	26	ОПК-1	Л1.1 Л2.1
Модуль 2 Безопасность компьютерных сетей (28+28)					
2.1	Лекция 6 Основные понятия, концепции и принципы информационной безопасности 1. Идентификация, аутентификация и авторизация 2. Модели информационной безопасности 3. Уязвимость, угроза, атака 4. Иерархия средств защиты от информационных угроз	Л6	2	ОПК-1	Л1.1 Л1.2
2.2	Практическое занятие №5 Модель угроз 1. Угроза, способы реализации угроз 2. Показатели уязвимости информации 3. Модель оценки ущерба от реализации угроз безопасности информации	Пз №5	4	ОПК-1	Л1.2 Л2.3
2.3	Лекция 7 Шифрование – базовая технология безопасности 1. Основные понятия и определения 2. Симметричное шифрование 3. Концепция асимметричного шифрования	Л7	2	ОПК-1	Л1.1 Л1.2
2.4	Практическое занятие №6 Криптографические алгоритмы 1. Шифры перестановки 2. Шифры замены 3. Поточные шифры	Пз №6	4	ОПК-1	Л1.1 Л2.1
2.5	Лекция 8 Технологии аутентификации, авторизации и управление доступом 1. Технологии аутентификации 2. Технологии управление доступом и авторизации 3. Системы аутентификации и управление доступом операционных систем	Л8	2	ОПК-1	Л1.1 Л1.2 Л2.2
2.6	Практическое занятие №7 Методы аутентификации	Пз №7	4	ОПК-1	Л1.1 Л2.1

	1. Аутентификация на знании 2. Аутентификация на основе обладания предметом 3. Аутентификация на воплощенных характеристиках				Л2.2
2.7	Лекция 9 Технологии безопасности на основе фильтрации и мониторинга трафика 1. Виды фильтрации. Стандартные и дополнительные правила фильтрации маршрутизаторов 2. Файерволы и функция NAT 3. Мониторинг трафика. Анализаторы протоколов	Л9	2	ОПК-1	Л1.1
2.8	Лекция 10 Атаки на транспортную инфраструктуру сети 1. Типы атак. Характеристики 2. Сетевая разведка 3. Безопасность маршрутизации на основе BGP 4. Технологии защищенного канала	Л10	2	ОПК-1	Л1.1 Л1.2
2.9	Лекция 11 Безопасность программного кода и сетевых служб 1. Уязвимости программного кода и вредоносные программы 2. Безопасность электронной почты 3. Облачные сервисы и их безопасность	Л11	2	ОПК-1	Л1.1 Л1.2
2.10	Практическое занятие №8 Мониторинг трафика 1. Контроль трафика сети 2. Управление трафиком	Пз №8	4	ОПК-1	Л1.1 Л2.1
2.12	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.	СР	28	ОПК-1	Л1.1 Л2.1
2.13	**Зачет**			ОПК-1	Л1.1 Л1.2 Л2.1 Л2.2
Итого – 108 часов					

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, В.П. Лось, Р. В. Мещеряков, Д. А. Шелупанов	Основы информационной безопасности	М.: Гор. линия-Телеком, 2011. - 558	Э3
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	1. AVAST Free Antivirus 2. Dr.Web Antivirus 3. Антивирус Касперского 4. ESET NOD32 Антивирус 5. Norton AntiVirus	Антивирусное ПО. Свободное, условно свободное или триал-версии
П.2	1. Wise Folder Hider 2. Secure Folders 3. Anvide Lock Folder 4. Folder Lock 5. Easy File Locker	Программное обеспечение по защите и сокрытию файлов и папок. Свободное, условно свободное или триал-версии.
П.3	1. TrustPort Tools 2. Cryptic Disk 3. Locker (скрытие файлов) 4. Max File Encryption 5. Secure Disk 6. Шифровальщик	Программное обеспечение по шифрованию, безвозвратному удалению, стеганографии. Свободное, условно свободное или триал-версии.

П.4	1. Hetman Partition Recovery 2. Active File Recovery 3. R-Studio 7.6 4. Auslogics File Recovery 5. Active UNDELETE 6. Recover My Files 7. R-Undelete 8. Handy Recovery 9. Ashampoo Undeleter	Программное обеспечение по восстановлению данных. Свободное, условно свободное или триал-версии.
П.5	1. Iperius Backup 2. FBackup 3. Backup4all 4. Uranium Backup Free 5. Simple Data Backup 6. Personal Backup 7. Back4Sure	Программное обеспечение по резервному копированию данных. Свободное, условно свободное или триал-версии.
П.6	MS Word – с лицензией	
П.7	Power Point – с лицензией	

6. Материально-техническое обеспечение дисциплины

6.1 МТО лекционных занятий	
1	Лекционная аудитория, оборудованная интерактивной доской, проектором
6.2 МТО практических занятий	
1	Компьютерная аудитория с выходом в интернет
6.3 МТО рубежных контролей, экзамена	
1	Компьютерная аудитория

7. Методические указания для обучающихся по освоению дисциплины

7.1 Указания по самостоятельной работе студента

Достижение целей эффективной подготовки студентов в вузах невозможно без их целеустремленной самостоятельной работы. При этом, безусловно, нельзя обойтись без живого общения и консультирования со стороны профессорско-преподавательского состава Самостоятельная работа студентов является составной частью учебной работы и имеет целью закрепление и углубление полученных знаний и навыков, поиск и приобретение новых знаний, в том числе с использованием автоматизированных обучающих курсов (систем), а также выполнение учебных заданий, подготовку к предстоящим занятиям, зачетам и экзаменам. Обязательным компонентом самостоятельной работы студентов является внеаудиторный практикум по иностранному языку.

Самостоятельная работа организуется преподавателями, обеспечивается и контролируется кафедрами. Она предусматривает, как правило, разработку рефератов, выполнение расчетно-графических, вычислительных работ, моделирования и других творческих заданий в соответствии с учебной программой (тематическим планом изучения дисциплины). Основная цель данного вида занятий состоит в обучении курсантов методам самостоятельной работы с учебным материалом.

Материал, подлежащий обработке на самостоятельных занятиях, намечается при разработке программы самостоятельной работы. Опыт, накопленный кафедрами в организации

самостоятельных занятий, что материал выделяемый на такие занятия, должен удовлетворять следующим требованиям:

- быть изложенным в учебнике достаточно полно и с примерами;
- обеспечиваться достаточным количеством литературы, учебных пособий. учебно-методических материалов, образцов техники
- содержать материал. углубляющий знания, полученные на лекции;
- осваивать проблемные еще не полностью решенные вопросы.

Проведению самостоятельной работы (как и любого другого вида занятий) должна предшествовать подготовка как преподавателя, так и обучаемых.

Постановку задачи обучаемым на проведение самостоятельного занятия преподаватель осуществляет на одном из занятия, предшествующему данному. Он разъясняет смысл занятия и указывает, что к нему студенты должны приготовить. Задание на самостоятельную работу должно быть выдано заблаговременно с тем, чтобы слушатели имели время на информационный поиск в библиотеке необходимых пособий.

Методику самостоятельной работы все обучаемые выбирают индивидуально, но методика достижения конечной цели может определяться преподавателем и включать: последовательность изучения и усвоения учебно-методического материала, пособий, руководств, наставлений, техники и т.д.; определение главного в изучаемом материале, материале, который необходимо законспектировать; просмотр учебных кинофильмов и их обсуждение; работу студентов по индивидуальным заданиям; опрос обучаемых в течении 7-10 минут с целью проверки усвоения главного из прочитанного материала.

При возникновении затруднений у обучаемых в разрешении вопросов задания преподавателю необходимо предусмотреть, чтобы каждый обучаемый мог получить оперативную консультацию по любому вопросу, если же при самостоятельной работе возникают затруднения по одному и тому же материалу (вопросу) у многих обучаемых, то желательно провести групповую консультацию.

Для контроля усвоения учебного материала целесообразно проводить в групповое собеседование или обсуждение изучаемого материала, проведение контрольных работ и т.п. Контрольные мероприятия при должной их организации позволяют не только оценивать знания материала, но и углубить и закрепить его у обучаемых.

Приветствуется использование компьютеров, которое:

- расширяет информационную баз) учебных занятий;
- повышает активность обучаемых, из пассивного получателя информации они превращаются в её добытчиков:
- способствует развитию способностей к анализу и обобщению, улучшает связанность, широту и глубину мышления;
- облегчает усвоение абстрактного материала, позволяет многое из него представить в виде конкретных образов;
- приучает к точности, аккуратности, последовательности действий способствует развитию самостоятельности.

Компьютерные технологии и программные продукты для выполнения самостоятельной работы по освоению учебного материала необходимо использовать в соответствии с указаниями методических разработок раздела 5 настоящей Рабочей программы.

Для более углубленного изучения материала по дисциплине целесообразно использовать учебные курсы сайта http://www.intuit.ru/ .

Таблица 7.1 – Учебный материал, выносимый на самостоятельное изучение студентам очной формы обучения

№	Темы, разделы, вынесенные на самостоятельную подготовку, вопросы для подготовки к практическим и лабораторным занятиям; курсовые работы, содержание контрольных работ; рекомендации по использованию литературы, ЭВМ и др.	Часов всего: 54	Неделя
Модуль 1 – 26 часа			
1	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).	4	1
2	Коммутируемые сети Ethernet.	4	2
3	Кодирование и мультиплексирование данных.	6	3-4
4	Беспроводная передача данных.	6	5-6
5	Технологии локальных сетей на разделяемой среде.	6	7-8
Модуль 2 – 28 часа			
6	Виртуальные частные сети.	4	9
7	Служба управления сетью.	4	10
8	Иерархия средств защиты от информационных угроз. Принципы защиты информационной системы.	6	11-12
9	Шифрование. Метод Диффи-Хелмана. Хеш-функции.	4	13
10	Атаки на транспортную инфраструктуру сети.	6	13-15
11	Облачные сервисы и их безопасность	4	16

Дополнения и изменения в рабочей программе