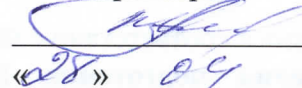


МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
Северо-Кавказский филиал
ордена Трудового Красного Знамени федерального государственного
бюджетного образовательного учреждения высшего образования
«Московский технический университет связи и информатики»

Утверждаю

Зам. директора по УР

 Н.А. Андреева
«28» 09 2026 г.

Рабочая программа дисциплины

Б1.В.06 Введение в профессию

Кафедра

Направление подготовки: **Информационная безопасность**
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/сем.
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	4	144/1
Контактная работа, в том числе (по семестрам, курсам):		54/1
Лекции		36/1
Лабораторных работ		
Практических занятий		18/1
Семинаров		
Самостоятельная работа		54/1
Контроль		36/1
Число контрольных работ (по курсам)		
Число КР (по семестрам, курсам)		
Число КП (по семестрам, курсам)		
Число зачетов с разбивкой по семестрам		
Число экзаменов с разбивкой по семестрам (курсам)		1/1

Программу составил:
К.т.н. доцент Маршаков Д.В.

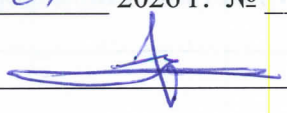
Рабочая программа дисциплины
«Введение в профессию»

Разработана в соответствии с ФГОС ВО:
направления подготовки **10.03.01 «Информационная безопасность»**, утвержденным
приказом Министерства науки и высшего образования Российской Федерации от 17 но-
ября 2020 г. N 1427

Составлена на основании учебных планов
направления **10.03.01 Информационная безопасность, профиль «Безопасность компью-
терных систем (по отрасли или в сфере профессиональной деятельности)»**, одобренного
Учёным советом СКФ МТУСИ, протокол № 8 от 31.03 2026г, и утвержденного
директором СКФ МТУСИ 31.03 2026 г.

Рассмотрена и одобрена на заседании кафедры
Информационная безопасность

Протокол от «28» 04 2026 г. № 9

И.О. Зав. кафедрой  Жуковский А.Г.

1. Цели изучения дисциплины

Целями изучения дисциплины "**Введение в профессию**" являются формирование у обучающихся 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 обучающегося способности решать профессиональные задачи в соответствии с **эксплуатационным** видом деятельности.

Результатом освоения дисциплины являются сформированные у обучающегося следующие компетенции:

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 при освоении академических дисциплин; - образовательную траекторию при изучении профильных дисциплин и саморазвития в сфере информационной безопасности.	
Уметь:	
- планировать собственное время при проведении исследований в области своей будущей профессиональной деятельности; - реализовывать траекторию саморазвития при решении базовых задач будущей профессиональной деятельности; - выстраивать траекторию саморазвития при планировании стратегий решения задач будущей профессиональной деятельности; - использовать методы самообучения при решении задач будущей профессиональной деятельности.	
Владеть:	
- навыками планирования своего времени при проведении расчетов типовых профессиональных задач; - навыками самообучения при реализации образовательной траектории в различных стратегиях решения задач будущей профессиональной деятельности; - навыками самоорганизации различных моделей поведения, необходимых для решения типовых профессиональных задач.	

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 – Информатика, Математика	
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Б1.О.27 Основы информационной безопасности
2	Б1.О.29 Методы и средства криптографической защиты информации
3	Б1.О.32 Основы управления информационной безопасностью

4. Структура и содержание дисциплины

4.1. Очная форма обучения, 4 года (всего 144 часа, из них 54 часа аудиторных)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
1	2	3	4	5	6
Курс 1, Семестр 1					
Модуль 1: Введение в информационную безопасность					
1.1	<u>Лекция 1. Профессия специалиста по защите информации</u> Понятие информационной безопасности. Кибербезопасность. Компетенции и роли в кибербезопасности. Профессиональные стандарты. Разделы кибербезопасности.	Лек.	4	УК-6	Л1.1 Л2.1 Л2.2
1.2	<u>Лекция 2. Исходные положения кибербезопасности</u> История развития. Общая характеристика принципов кибербезопасности. Угрозы безопасности в компьютерных системах. Политика и модели безопасности.	Лек.	4	УК-6	Л1.1 Л1.2 Л2.1 Л2.2
1.3	<u>Лекция 3. Парольная защита информации</u> Принцип парольной защиты. Возможности обхода парольной защиты. Повышение эффективности. Достоинства и недостатки.	Лек.	4	УК-6	Л1.1 Л1.3
1.4	<u>Лекция 4. Системы идентификации и аутентификации</u> Понятия идентификации, аутентификации, авторизации. Учетная запись. Электронные идентификаторы. Системы биометрической идентификации.	Лек.	4	УК-6	Л1.1 Л1.2
1.5	<u>Лекция 5. Системы защиты от несанкционированного доступа</u> Модели управления доступом. Мандатная, дискреционная, ролевая модели разграничения доступа. HRU-модель. Модель Take-Grant.	Лек.	4	УК-6	Л1.1 Л1.2
1.6	Практическая работа 1. Исследование парольной защиты информации	ПЗ	4	УК-6	Л1.1 Л1.2 Л3.1
1.7	Практическая работа 2. Механизмы разграничения доступа	ПЗ	4	УК-6	Л1.1 Л2.3 Л3.1
1.8	Практическая работа 3. Модели управления доступом	ПЗ	4	УК-6	Л1.1 Л2.3 Л3.1
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.	СРС	24	УК-6	Л1.1 Л2.1
Модуль 2: Математические основы компьютерной безопасности					
2.1	<u>Лекция 6. Криптографические методы защиты информации</u> Криптография как наука. Роль криптографии в кибербезопасности. Классификация средств криптографической защиты ин-	Лек.	4	УК-6	Л1.1 Л1.2 Л1.3

	формации. Краткие сведения о криптоанализе.				
2.2	Лекция 7. Классические методы шифрования информации Математические основы криптографии. Модель традиционного шифрования. Требования к криптографическим системам. Методы подстановки и перестановки.	Лек.	4	УК-6	Л1.1 Л1.2 Л1.3
2.3	Лекция 8. Криптосистемы с закрытым ключом Блочные шифры. Шифр DES. Шифр AES. Шифр ГОСТ 34.12-2018. Основные режимы функционирования блочных шифров.	Лек.	4	УК-6	Л1.1 Л1.2 Л1.3
2.4	Лекция 9. Криптосистемы с открытым ключом Общая схема защиты информации. Система Диффи-Хеллмана. Элементы теории чисел. Шифр Шамира. Шифр Эль-Гамала. Шифр RSA.	Лек.	4	УК-6	Л1.1 Л1.2 Л1.3
2.5	Практическая работа 4. Знакомство с киберполигоном Amprige	ПЗ	2	УК-6	Л1.1 Л1.2 Л3.1
2.6	Практическая работа 5. Выявление инцидентов информационной безопасности	ПЗ	2	УК-6	Л1.1 Л1.2 Л3.1
2.7	Практическая работа 6. Защита базы данных предприятия	ПЗ	2	УК-6	Л1.1 Л1.2 Л3.1
2.13	Электронная подпись. Криптографические протоколы. Случайные числа в криптографии. Стеганография и стегоанализ.	СРС	30	УК-6	Л1.1 Л1.2 Л1.3 Л2.3
	Экзамен		36	УК-6	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.1
Итого – 144 часа					

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	Шаньгин, В. Ф.	Информационная безопасность и защита информации	Саратов : Профобразование, 2024. — 702 с.	Э1
Л1.2	Трушин В.А., Котов Ю.А., Левин Л.С., Донской К.А.	Введение в информационную безопасность и защиту информации : учебное пособие	Новосибирск: Новосибирский государственный технический университет, 2017. – 132 с.	Э2
Л1.3	Хасанов, Р. И.	Основы стеганографии : учебное пособие	Оренбург : Оренбургский государственный университет, ЭБС АСВ, 2016. — 102 с.	Э3
5.1.2 Дополнительная литература				
Код	Авторы,	Заглавие	Издательство,	Кол.

	составители		год	
Л2.1	Зырянова, Т. Ю.	Основы криптографии : учебное пособие	Екатеринбург : Уральский государственный университет путей сообщения, 2023. — 83 с.	Э4
Л2.2	Гисин, В. Б.	Криптография и распределенные реестры : учебное пособие	Москва: Прометей, 2022. — 186 с.	Э5
Л2.3	Башлы, П. Н., А. В. Бабаш, Е. К. Баранова	Информационная безопасность и защита информации : учебное пособие	Москва : Евразийский открытый институт, 2012. — 311 с.	Э6
5.1.3 Учебно-методическое обеспечение				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л3.1	С. А. Омарова, К. А. Исакова, Н.А. Тойганбаева	Информационная безопасность и защита информации : учебно-методический комплекс	Алматы : Нур-Принт, 2012. — 98 с.	Э7
5.2 Электронные образовательные ресурсы				
Э1	https://www.iprbookshop.ru/145912.html			
Э2	https://www.iprbookshop.ru/91329.html			
Э3	https://www.iprbookshop.ru/78809.html			
Э4	https://www.iprbookshop.ru/149716.html			
Э5	https://www.iprbookshop.ru/153506.html			
Э6	https://www.iprbookshop.ru/10677.html			
Э7	https://www.iprbookshop.ru/67055.html			
5.3 Информационно-справочные системы и профессиональные базы данных				
5.3.1	Консультант Плюс – https://www.consultant.ru/			
5.3.2	Гарант – https://www.garant.ru/			
5.3.2	Консорциум Кодекс – https://docs.cntd.ru/			
5.3.3	Научная электронная библиотека – https://www.elibrary.ru/			
5.3.4	Профессиональная база данных: Федеральный портал «Российское образование»: [Электронный ресурс] – Режим доступа: http://www.edu.ru/ (открытый доступ)			
5.3.5	Профессиональная база данных: Федеральный центр информационно-образовательных ресурсов: [Электронный ресурс] – Режим доступа: http://fcior.edu.ru/ (открытый доступ)			
5.3.6	Национальный открытый университет «ИНТУИТ» - https://intuit.ru/			
5.3.7	Электронный ресурс http://www.securitylab.ru/			
5.4 Программное обеспечение				
П.1	Linux (свободное ПО)			
П.2	LibreOffice (свободное ПО)			
П.3	Яндекс Браузер (свободное ПО)			
П.4	Secret Net Studio			

6. Материально-техническое обеспечение дисциплины

6.1 МТО лекционных занятий	
1	Лекционная аудитория, оснащенная интерактивной доской, проектором, ПК (ноутбуком), экраном.
6.2 МТО лабораторных работ и практических занятий	
1	Лаборатория «Программно-аппаратные средства защиты информации», укомплектованная специализированной мебелью, оснащенную программно-аппаратными комплексами защиты информации, включающими в том числе средства криптографической защиты информации,
2	Лаборатория «Технической защиты информации», укомплектованная специализированной мебелью, оснащенная техническими средствами защиты информации

3	Учебные аудитории, оборудованные компьютерной техникой, с возможностью подключения к сети «Интернет», и обеспечением доступа в электронную информационно-образовательную среду СКФ МТУСИ
6.3 МТО рубежных контролей, зачетов, экзаменов	
1	Учебные аудитории, оборудованные компьютерной техникой с возможностью выхода в локальную сеть Филиала и Интернет.
6.4 МТО самостоятельной работы обучающихся	
1	Помещение для самостоятельной работы обучающихся оснащено компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду СКФ МТУСИ

7. Оценочные материалы	
Оценочные материалы и перечень видов оценочных средств текущего контроля и промежуточной аттестации представлены в Приложении 1 к рабочей программе дисциплины.	

8. Методические рекомендации для обучающихся по освоению дисциплины	
Методические рекомендации по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины.	

9. Особенности реализации дисциплины (модуля) при обучении инвалидов и лиц с ограниченными возможностями здоровья

Рабочая программа дисциплины (модуля) при необходимости может быть адаптирована для обучения (в том числе с применением дистанционных образовательных технологий) лиц с ограниченными возможностями здоровья, инвалидов. Для этого требуется заявление обучающихся, являющихся лицами с ограниченными возможностями здоровья, инвалидами, или их законных представителей и рекомендации психолого-медико-педагогической комиссии. При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков.

Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания.

Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т.д.).

Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь.

Текущий контроль успеваемости осуществляется в устной форме.

При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).

10. Дополнения и изменения в Рабочей программе

Лист актуализации рабочей программы дисциплины «Б1.В.06 Введение в профессию» для использования в 20__/20__ учебном году

Утверждаю

Зам. директора по УР _____
«__» _____ 20__ г.

Направление: 10.03.01 Информационная безопасность

Профиль: Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)

Форма обучения: очная

(Возможны следующие варианты):

а) Рабочая программа действует без изменений.

б) В рабочую программу вносятся следующие изменения:

1)

2)

3)

Разработчик (и): _____
(ФИО, ученая степень, ученое звание)

«__» _____ 20__ г.

Рабочая программа пересмотрена и одобрена на заседании кафедры ИБ

Протокол № _____ от «__» _____ 20__ г.

Заведующий кафедрой _____

Оценочные материалы для проведения текущего контроля и промежуточной аттестации по дисциплине

1. Оценочные материалы для проведения промежуточной аттестации по дисциплине

1.1 Шкала оценивания компетенций

Шкала оценивания компетенций		
Оценка	Уровень освоения компетенции	Критерии оценивания
«Отлично»	Высокий уровень	Обучающийся показывает всестороннее, систематическое и глубокое знание основного и дополнительного учебного материала, умеет свободно выполнять задания, предусмотренные программой; усвоил основную и знаком с дополнительной рекомендованной литературой; может объяснить взаимосвязь основных понятий дисциплины в их значении для последующей профессиональной деятельности; проявляет творческие способности в понимании, изложении и использовании учебного материала.
«Хорошо»	Повышенный уровень	Обучающийся показывает достаточный уровень знаний в пределах основного учебного материала, без существенных ошибок выполняет предусмотренные в программе задания; усвоил основную литературу, рекомендованную в программе; способен объяснить взаимосвязь основных понятий дисциплины при дополнительных вопросах преподавателя. Допускает не существенные погрешности в ответах, устраняет их без помощи преподавателя.
«Удовлетворительно»	Пороговый уровень	Обучающийся показывает знания основного учебного материала в минимальном объеме, необходимом для дальнейшей учебы; справляется с выполнением заданий, предусмотренных программой, допуская при этом большое количество не принципиальных ошибок; знаком с основной литературой, рекомендованной программой. Допускает существенные погрешности в ответах, но обладает необходимыми знаниями для их устранения под руководством преподавателя.
«Неудовлетворительно»	Минимальный уровень не достигнут	Обучающийся обнаруживает пробелы в знаниях основного учебного материала, допускает принципиальные ошибки в выполнении предусмотренных программой заданий, не знаком с рекомендованной литературой, не может исправить допущенные ошибки. Как правило, оценка «неудовлетворительно» ставится обу-

		чающимся, которые не могут продолжить обучение или приступить к профессиональной деятельности по окончании вуза без дополнительных занятий по соответствующей дисциплине.
--	--	---

1.2 Показатели, критерии и шкалы оценивания компетенций

Показатели компетенции	Критерии оценивания	Шкала оценивания
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 при освоении академических дисциплин;	Контрольная работа 1	Модуль 1 0–20 «Неудовлетворительно» - 0-4 «Удовлетворительно» - 5-10 «Хорошо» - 11-15 «Отлично» - 16-20
- образовательную траекторию при изучении профильных дисциплин и саморазвития в сфере информационной безопасности.	Контрольная работа 2	Модуль 2 0–20 «Неудовлетворительно» - 0-4 «Удовлетворительно» - 5-10 «Хорошо» - 11-15 «Отлично» - 16-20
Уметь:		
- планировать собственное время при проведении исследований в области своей будущей профессиональной деятельности;	Практическое занятие 1	Модуль 1 0–10 «Неудовлетворительно» - 0-4 «Удовлетворительно» - 5-6 «Хорошо» - 7-8 «Отлично» - 9-10
- реализовывать траекторию саморазвития при решении базовых задач будущей профессиональной деятельности;	Практическое занятие 3	Модуль 1 0–10 «Неудовлетворительно» - 0-4 «Удовлетворительно» - 5-6 «Хорошо» - 7-8 «Отлично» - 9-10
- выстраивать траекторию саморазвития при планировании стратегий решения задач будущей профессиональной деятельности;	Практическое занятие 5	Модуль 2 0–10 «Неудовлетворительно» - 0-4 «Удовлетворительно» - 5-6 «Хорошо» - 7-8 «Отлично» - 9-10
- использовать методы самообучения при решении задач будущей профессиональной деятельности.	Практическое занятие 6	Модуль 2 0–10 «Неудовлетворительно» - 0-4 «Удовлетворительно» - 5-6 «Хорошо» - 7-8 «Отлично» - 9-10

Владеть:		
- навыками планирования своего времени при проведении расчетов типовых профессиональных задач;	Практическое занятие 2	Модуль 1 0–10 «Неудовлетворительно» - 0-4 «Удовлетворительно» - 5-6 «Хорошо» - 7-8 «Отлично» - 9-10
- навыками самообучения при реализации образовательной траектории в различных стратегиях решения задач будущей профессиональной деятельности;	Практическое занятие 3	Модуль 1 0–10 «Неудовлетворительно» - 0-4 «Удовлетворительно» - 5-6 «Хорошо» - 7-8 «Отлично» - 9-10
- навыками самоорганизации различных моделей поведения, необходимых для решения типовых профессиональных задач.	Практическое занятие 4	Модуль 2 0–10 «Неудовлетворительно» - 0-4 «Удовлетворительно» - 5-6 «Хорошо» - 7-8 «Отлично» - 9-10
	Экзамен	0-100 баллов «Неудовлетворительно» - 0-40 «Удовлетворительно» - 41-60 «Хорошо» - 61-80 «Отлично» - 81-100

1.3 Оценочные материалы: типовые контрольные задания, иные материалы

1.3.1 Оценочные материалы текущего контроля для очной формы обучения

Модуль 1 (50 баллов):

Модуль содержит 10 лекционных и 3 практических занятия. Знание лекционного материала оценивается по контрольной работе, состоящей из двух вопросов, максимальное количество баллов за контрольную работу составляет 20. За выполненные и защищенные практические занятия и лабораторные работы обучающийся получает максимум 30 баллов. Общее максимальное количество баллов за модуль 1 составляет 50.

Вопросы для контрольной работы 1 (УК-6):

1. Основные понятия информационной безопасности: конфиденциальность, целостность, доступность, угроза, уязвимость, риск.
2. Информационная безопасность и кибербезопасность. Особенности и отличия.
3. Профстандарты в области информационной безопасности. Трудовые функции специалиста по безопасности компьютерных систем и сетей.
4. Знания и навыки, необходимые администратору по обеспечению безопасности информации.
5. Виды и отличительные особенности соревнований в области кибербезопасности.
6. Роль парольной защиты в обеспечении безопасности. Методы оценки безопасного времени функционирования пароля.
7. Характеристики парольной защиты. Методы обхода парольной защиты.

8. Политика безопасности: понятие, виды. Достоверная вычислительная база. Принципы реализации политики безопасности.
9. Понятие и назначение модели безопасности. Модель дискреционного доступа. Модель безопасности Белла-ЛаПадулы.
10. Модель разграничения доступа Харрисона-Руззо-Ульмана.
11. Модель разграничения доступа Take-Grant.
12. Понятие и назначение модели безопасности. Ролевая модель контроля доступа. Системы разграничения доступа: назначение и примеры.
13. Классификация систем идентификации и аутентификации. Электронные идентификаторы: виды и особенности.
14. Классификация систем идентификации и аутентификации. Биометрические идентификаторы: виды и особенности.
15. Классификация систем идентификации и аутентификации. Особенности комбинированных систем идентификации и аутентификации.

Практическое занятие №1. Исследование парольной защиты информации.

Контрольные вопросы (УК-6):

1. Дайте определение понятию идентификации. Аутентификации.
2. Дайте определение паролю.
3. Перечислите основные виды атак на пароль и принципы их работы.
4. Что такое словарь? Какие виды словарей существуют?
5. Каким основным характеристикам должен удовлетворять надежный пароль?
6. От какого параметра пароля наибольшим образом зависит его надежность?

Практическое занятие №2. Механизмы разграничения доступа.

Контрольные вопросы (УК-6):

1. Для чего предназначено СЗИ Secret Net Studio?
2. Перечислите основные возможности СЗИ Secret Net Studio.
3. В каких режимах может производиться развертывание системы Secret Net Studio?
4. Какие механизмы разграничения доступа реализованы в СЗИ Secret Net Studio?
5. Что такое замкнутая программная среда?
6. Каким образом осуществляется задание пользователю персонального идентификатора в СЗИ Secret Net Studio?

Практическое занятие №3. Модели управления доступом.

Контрольные вопросы (УК-6):

1. Что такое модель управления доступом?
2. Какие основные типы моделей управления доступом существуют?
3. В чем разница между мандатной и дискреционной моделями управления доступом?
4. Модель разграничения доступа Белла-ЛаПадулы.
5. Модель разграничения доступа Харрисона-Руззо-Ульмана.
6. Модель разграничения доступа Take-Grant.

Модуль 2 (50 баллов):

Модуль содержит 8 лекционных и 3 практических занятия. Знание лекционного материала оценивается по контрольной работе, состоящей из двух вопросов, максимальное количество баллов за контрольную работу составляет 20. За выполненные и защищенные практические занятия и лабораторные работы обучающийся получает максимум 30 баллов. Общее максимальное количество баллов за модуль 2 составляет 50.

Вопросы для контрольной работы 2 (УК-6):

1. Криптография как наука. Роль криптографии в кибербезопасности.
2. Блочные и поточные шифры.
3. Классические шифры подстановки и перестановки.
4. Классификация и особенности средств криптографической защиты информации. Симметричное шифрование: алгоритмы, стандарты, особенности.
5. Особенности криптосистемы DES. Шифр AES.
6. Особенности криптосистемы ГОСТ 34.12-2018. Основные режимы функционирования блочных шифров.
7. Классификация и особенности средств криптографической защиты информации. Асимметричное шифрование: алгоритмы, стандарты, особенности.
8. Схема Диффи-Хеллмана. Шифр Эль-Гамала.
9. Особенности криптосистемы RSA.
10. Виды злоумышленных действий, возможных в отсутствие электронной подписи.
11. Особенности применения электронной подписи (ЭП). Алгоритмы ЭП. Сертификаты ЭП.
12. Примеры криптопровайдеров.

Практическое занятие №4. Знакомство с киберполигоном Ampire.

Контрольные вопросы (УК-6):

1. Для чего предназначен программный комплекс Ampire?
2. Как происходит организация процесса отражения атаки?
3. Своими словами объясните: для чего предназначена логическая схема сценария.
4. Что значит каждый индикатор на дашборде при прохождении тренировки?
5. Для чего предназначены карточки инцидентов? Поясните, как их нужно заполнять.
6. Для чего предназначены карточки Cyber Kill Chain?
7. В чём роль лидера группы реагирования?

Практическое занятие №5. Выявление инцидентов информационной безопасности.

Контрольные вопросы (УК-6):

1. Что вы уже знаете про средства обнаружения вторжений?
2. Кратко расскажите о сетевом сенсоре VIPNET IDS NS.
3. Кратко расскажите о TIAS.
4. Кратко расскажите о SecOnion.
5. Что из себя представляет атака Brute-force?
6. Назовите виды систем обнаружения вторжений.
7. Что необходимо сделать, чтобы команда не записалась в .bash_history??

Практическое занятие №6. Защита базы данных предприятия.

Контрольные вопросы (УК-6):

1. Объясните своими словами что такое CMS?
2. Назовите основные функции CMS.
3. Что такое уязвимости сайтов?
4. Приведите примеры уязвимостей сайтов.
5. Объясните своими словами суть уязвимости Drupalgeddon2 (CVE-2018-7600).
6. Что такое SSH и Telnet?
7. Перечислите основные отличия SSH от Telnet.

1.3.2 Вопросы, выносимые на экзамен по дисциплине (УК-6) (промежуточная аттестация):

1. Основные понятия информационной безопасности: конфиденциальность, целостность, доступность, угроза, уязвимость, риск.
2. Информационная безопасность и кибербезопасность. Особенности и отличия.
3. Профстандарты в области информационной безопасности. Трудовые функции специалиста по безопасности компьютерных систем и сетей.
4. Знания и навыки, необходимые администратору по обеспечению безопасности информации.
5. Виды и отличительные особенности соревнований в области кибербезопасности.
6. Роль парольной защиты в обеспечении безопасности. Методы оценки безопасного времени функционирования пароля.
7. Характеристики парольной защиты. Методы обхода парольной защиты.
8. Политика безопасности: понятие, виды. Достоверная вычислительная база. Принципы реализации политики безопасности.
9. Понятие и назначение модели безопасности. Модель дискреционного доступа. Модель безопасности Белла-ЛаПадулы.
10. Модель разграничения доступа Харрисона-Руззо-Ульмана.
11. Модель разграничения доступа Take-Grant.
12. Понятие и назначение модели безопасности. Ролевая модель контроля доступа. Системы разграничения доступа: назначение и примеры.
13. Классификация систем идентификации и аутентификации. Электронные идентификаторы: виды и особенности.
14. Классификация систем идентификации и аутентификации. Биометрические идентификаторы: виды и особенности.
15. Классификация систем идентификации и аутентификации. Особенности комбинированных систем идентификации и аутентификации.
16. Криптография как наука. Роль криптографии в кибербезопасности.
17. Блочные и поточные шифры.
18. Классические шифры подстановки и перестановки.
19. Классификация и особенности средств криптографической защиты информации. Симметричное шифрование: алгоритмы, стандарты, особенности.
20. Особенности криптосистемы DES. Шифр AES.
21. Особенности криптосистемы ГОСТ 34.12-2018. Основные режимы функционирования блочных шифров.
22. Классификация и особенности средств криптографической защиты информации. Асимметричное шифрование: алгоритмы, стандарты, особенности.
23. Схема Диффи-Хеллмана. Шифр Эль-Гамала.
24. Особенности криптосистемы RSA.
25. Виды злоумышленных действий, возможных в отсутствие электронной подписи.
26. Особенности применения электронной подписи (ЭП). Алгоритмы ЭП. Сертификаты ЭП.
27. Примеры криптопровайдеров.

2. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Предусмотрены следующие виды контроля:

- текущий контроль по каждому модулю – в форме написания контрольной работы для оценки теоретических знаний;
- текущий контроль по каждому модулю – в форме отчетов по практическим занятиям для оценки практических навыков;
- промежуточная аттестация по дисциплине – в форме экзамена.

Текущий контроль успеваемости в форме защиты практических проводится в два этапа:

- 1-й этап: допуск к выполнению практической работы – проводится в форме письменной «летучки» (5-10 мин) с целью контроля знаний обучающихся теоретической части практической работы и готовности к выполнению практических исследований;

- 2-й этап выполняется по окончании каждого практического занятия в форме индивидуального собеседования по выполненным исследованиям или расчетам. Проводится с целью контроля закрепления теоретической части материала и степени отработки обучающимся практических навыков исследования на аппаратуре.

Контрольные работы выполняются в виде короткого письменного ответа на один вопрос, изученный на предыдущей лекции в начале каждой последующей лекции. Ответ на вопрос дается в течение 5-10 минут. Таким образом, после лекционного курса каждого модуля формируется общая оценка за теоретические знания.

С целью повышения качества обучения за счет побуждения обучающихся к активной текущей учебной работе, четкого и оперативного контроля всего хода учебного процесса, снижения роли случайных и субъективных факторов при оценивании учебной деятельности обучающихся в образовательном процессе реализована модульно-рейтинговая система.

Правила ее использования прописаны в «Положении об МРС».

Набранные обучающимися в рамках текущего контроля баллы могут быть переведены в оценку:

- «неудовлетворительно» - от 0 до 40 от максимального количества баллов;
- «удовлетворительно» - от 41 до 60 максимального количества баллов;
- «хорошо» - от 61 до 80 максимального количества баллов;
- «отлично» - от 81 до 100 максимального количества баллов.

Соотношения максимального количества баллов, полученных обучающимся по блокам модулей, показаны в Таблице 1.

Таблица 1 - Распределение баллов по блокам модулей дисциплины

Модуль	Всего баллов (Максимальное значение)	Теоретический блок (Контрольная работа)	Практический блок (Рас- пределение баллов по за- нятиям)
Модуль 1	50	20	30
Модуль 2	50	20	30
Экзамен	100	100	

Теоретический блок оценивается по результатам контрольной работы. Практический блок оценивается по результатам выполнения заданий на практических занятиях.

На экзамене производится оценка тех компетенций, которые должны быть в той или иной форме освоены в процессе изучения. Рекомендуются формировать вопросы в экзаменационных билетах таким образом, чтобы преподаватель смог оценить все компетенции данной дисциплины.

3. Промежуточная аттестация

Промежуточная аттестация проводится в форме экзамена.

Экзамен проводится по расписанию промежуточной аттестации в устном виде по экзаменационным билетам. Результаты аттестации заносятся в ведомость и зачетную книжку обучающегося.

Образец экзаменационного билета

	МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образова- тельного учреждения высшего образования «Московский технический университет связи и информа- тики»	Утверждаю И.О.зав. кафедрой «ИБ» _____ А.Г.Жуковский «___» _____ 20___ г.
Направление подготовки: 10.03.01 Информационная безопасность Курс: 1 Дисциплина: Введение в профессию		
Билет №1 1. Основные понятия информационной безопасности: конфиденциальность, целостность, до- ступность, угроза, уязвимость, риск. 2. Криптография как наука. Роль криптографии в кибербезопасности. к.т.н. доцент Маршаков Д.В. _____ Маршаков Д.В. «___» _____ 20___ г.		

Один комплект отпечатанных экзаменационных билетов, подписанных преподавателем кафедры и утвержденных заведующим кафедрой хранится у заведующего кафедрой, другой комплект – у преподавателя, ведущего дисциплину.

4. ТЕСТОВЫЕ ЗАДАНИЯ ПО ДИСЦИПЛИНЕ (УК-6)

Тестовые задания позволяют оценить уровень сформированности 1-й компетенции УК-6.

Задания распределены по блокам в соответствии с уровнем сложности. Каждый блок содержит номер задания, и текст задания.

Базовый уровень содержит примерно 50% заданий.

Он формируется из заданий с выбором одного или нескольких верных ответов из предложенных или воспроизведения фактического материала (терминология, факты, классификация, параметры и др.);

Повышенный уровень в среднем составляет 35 % заданий.

В нем используются задания на сопоставление, сравнение, установление последовательности;

Высокий уровень в среднем составляют – 15 % заданий.

В задании используются: решения нетиповых задач, алгоритмы, доказательства, задания с развернутым ответом – определения, перечисление, изображение схемы, структуры и др.

Количество заданий компетенции равно 20.

Один комплект тестовых вопросов с указанием правильных ответов хранится у заведующего кафедрой, другой комплект – у преподавателя, ведущего дисциплину.

УК-6. Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни.

БЛОК А (базовый уровень) – Задание с выбором одного или нескольких верных ответов из предложенных

Инструкция по тестам Блока А: Прочитайте текст и выберите один или несколько правильных ответов

№	Дисциплина	Тексты заданий
1	Б1.В.06 Введение в профессию	Соревнования по «этичному хакингу», в которых участники ищут уязвимости и решают задачи по практической информационной безопасности: 1. СТФ 2. Хакатон 3. Квиз 4. Квест
2	Б1.В.06 Введение в профессию	В общем случае пароль представляет собой: 1. Строку символов, служащую в качестве аутентификатора пользователя 2. Цифровой код, служащий в качестве идентификатора пользователя 3. Совокупность идентификатора и аутентификатора субъекта 4. Битовую строку установленной длины, полученную с помощью определенного алгоритма хэширования
3	Б1.В.06 Введение в профессию	К электронным средствам идентификации и аутентификации относятся: 1. Идентификаторы iButton 2. Сканеры отпечатков пальцев 3. Бесконтактные смарт-карты 4. Считыватель радужной оболочки глаза 5. USB-ключи и токены
4	Б1.В.06 Введение в профессию	К биометрическим средствам идентификации и аутентификации относятся: 1. Сканеры отпечатков пальцев 2. Идентификаторы iButton 3. Бесконтактные смарт-карты 4. Токены 5. Считыватель радужной оболочки глаза
5	Б1.В.06 Введение в профессию	Мандатное управление доступом основано на: 1. Обеспечении доступа к защищаемым объектам в соответствии со списками пользователей (субъектов), в соответствии с содержимым которых вычисляются права на доступ к объекту для каждого пользователя 2. Контроле доступа субъектов к объектам на основе типов их активностей в системе

№	Дисциплина	Тексты заданий
		3. Назначении метки конфиденциальности для информации, содержащейся в объектах, и выдаче официальных допуска субъектам на обращение к информации такого уровня конфиденциальности
6	Б1.В.06 Введение в профессию	Дискреционная модель доступа: 1. Основана на назначении метки конфиденциальности для информации, содержащейся в объектах, и выдаче официальных разрешений субъектам на обращение к информации такого уровня конфиденциальности 2. Обеспечивает доступ к защищаемым объектам в соответствии со списками субъектов, в соответствии с содержанием которых вычисляются права на доступ к объекту для каждого пользователя. 3. Контролирует доступ субъектов к объектам на основе их действий и обязанностей, связанных с определенным им видом деятельности
7	Б1.В.06 Введение в профессию	Процедура авторизации пользователя представляет собой: 1. Действия по присвоению субъектам и объектам доступа идентификаторов или по сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов 2. Действия по проверке подлинности субъекта доступа в автоматизированной информационной системе 3. Предоставление субъекту прав на доступ, а также предоставление доступа в соответствии с установленными правами на доступ 4. Регистрация действий пользователя в системе, включая его попытки доступа к ресурсам
8	Б1.В.06 Введение в профессию	В алгоритмах блочного шифрования информация разбивается на блоки длиной: 1. 16 бит 2. 32 бита 3. 64 бит 4. 128 бит 5. 256 бит
9	Б1.В.06 Введение в профессию	К алгоритмам шифрования с закрытым ключом относятся: 1. RSA 2. AES 3. Twofish 4. ГОСТ 34.12-2018 5. Diffie–Hellman
10	Б1.В.06 Введение в профессию	К алгоритмам шифрования с открытым ключом относятся: 1. RSA 2. Elgamal 3. Blowfish 4. ГОСТ 34.12-2018 5. Diffie–Hellman

БЛОК Б (повышенный уровень) – Задание закрытого типа на установление соответствия
Инструкция: Прочитайте текст и установите соответствие

№	Дисциплина	Тексты заданий
11	Б1.В.06 Введение в профессию	Соотнесите термины с их определениями: 1. Уязвимость системы 2. Риск 3. Угроза информационной безопасности А. Свойство информационной системы, обуславливающее возможность реализации угроз безопасности обрабатываемой в ней информации Б. Потенциальная возможность того, что уязвимость будет использоваться для создания угрозы активу или группе активов, приводящей к ущербу для организации В. Совокупность факторов и условий, создающих опасность нарушения информационной безопасности, вызывающую или способную вызвать негативные последствия
12	Б1.В.06 Введение в профессию	Соотнесите термины с их определениями: 1. Конфиденциальность 2. Доступность 3. Целостность

№	Дисциплина	Тексты заданий
		А. Состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право Б. Состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно В. Состояние информации, при котором отсутствует любое её изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право
13	Б1.В.06 Введение в профессию	Для приведенных сценариев атаки на пароль укажите их названия. Сценарии атаки на пароль: 1. Перебор вариантов комбинаций, составленных на основе индивидуальных данных пользователя 2. Перебор общеизвестных слов естественного языка 3. Перебор всех возможных вариантов пароля определенной длины 4. Перебор всех возможных вариантов пароля на основе заданного шаблона Названия сценариев: А. Атака по персональному словарю Б. Атака по словарю В. Брутфорс Г. Атака по маске
14	Б1.В.06 Введение в профессию	Соотнесите понятия с их определениями: 1. Объектом доступа называется... 2. Субъектом доступа является... 3. Системой разграничения доступа называется... А. Единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа Б. Процесс, действия которого регламентируются правилами разграничения доступа В. Совокупность реализуемых правил разграничения доступа в средствах вычислительной техники или автоматизированных системах

БЛОК Б (повышенный уровень) – Задание закрытого типа на установление последовательности

Инструкция: Прочитайте текст и установите правильную последовательность

№	Дисциплина	Тексты заданий
15	Б1.В.06 Введение в профессию	Расставьте правильно последовательность действий при входе в защищённую систему: 1. Идентификация 2. Авторизация 3. Аутентификация
16	Б1.В.06 Введение в профессию	Расположите следующие криптографические алгоритмы в хронологическом порядке их появления: 1. Шифр Цезаря 2. AES 3. DES 4. RSA
17	Б1.В.06 Введение в профессию	Укажите последовательность действий злоумышленника по отношению к защищаемой системе: 1. Обнаружение уязвимости 2. Проведение атаки 3. Формирование угрозы

БЛОК В (высокий уровень) – Задание открытого типа с развернутым ответом

Инструкция: Прочитайте текст и запишите обоснованный ответ

№	Дисциплина	Тексты заданий
18	Б1.В.06 Введение в профессию	Напишите название термина. Злоумышленное действие с электронным документом, при котором абонент А заявляет, что не посылал сообщения абоненту В, хотя на самом деле послал, называется _____.

№	Дисциплина	Тексты заданий
19	Б1.В.06 Введение в профессию	Напишите название термина. Злоумышленное действие с электронным документом, при котором абонент С посылает документ абоненту В от имени абонента А, называется _____.
20	Б1.В.06 Введение в профессию	Напишите название термина. Злоумышленное действие с электронным документом, при котором абонент В изменяет или формирует новый документ и заявляет, что получил его от абонента А, называется _____.

Система оценивания выполнения тестовых заданий по компетенции УК-6

Номер задания	Указания по оцениванию	Результат оценивания (баллы, полученные за выполнение задания/характеристика правильности ответа)
Задания 1-10	Задания с выбором одного или нескольких верных ответов из предложенных считается верным, если правильно указана цифра или цифры, означающие верные ответы.	Совпадение с верным ответом оценивается 1 баллом; неверный ответ или его отсутствие - 0 баллов.
Задания 11-14	Задания закрытого типа на установление соответствия считается верным, если правильно установлены все соответствия (позиции из одного столбца верно сопоставлены с позициями другого)	Полное совпадение с верным ответом оценивается 1 баллом; неверный ответ или его отсутствие - 0 баллов.
Задания 15-17	Задания закрытого типа на установление последовательности считается верным, если правильно указана вся последовательность цифр	Полное совпадение с верным ответом оценивается 1 баллом; если допущены ошибки или ответ отсутствует - 0 баллов.
Задания 18-20	Задание открытого типа с развернутым ответом считается верным, если ответ совпадает с эталонным по содержанию и полноте.	Полный правильный ответ на задание оценивается 1 баллом. Если в ответе используются перечисления, то различный порядок следования правильных ответов в перечислении не считается ошибкой. Если допущена ошибка, ответ не полный, неправильный или отсутствует - 0 баллов.

Методические рекомендации по освоению дисциплины

1. Методические рекомендации преподавателю

Перед началом изучения дисциплины преподаватель должен ознакомить обучающихся с рабочей программой и оценочными материалами по дисциплине, с видами учебной и самостоятельной работы, перечнем литературы и интернет-ресурсов, с формами текущей и промежуточной аттестации, с критериями оценки качества знаний для итоговой оценки по дисциплине.

При проведении лекций, преподаватель:

- 1) формулирует тему и цель занятия, объявляет учебные вопросы;
- 2) излагает основные теоретические положения;
- 3) с помощью технических средств обучения и/или под запись дает определения основных понятий, расчетных формул;
- 4) проводит примеры из отечественного и зарубежного опыта, дает текущие статистические данные для наглядного и образного представления изучаемого материала;
- 5) в конце занятия выдает вопросы для самостоятельного изучения.

На занятиях лабораторного цикла следует обратить внимание на соответствие выбираемых обучающимся средств выполнения решаемым в работе задачам.

Каждая лабораторная работа должна быть оформлена и защищена в соответствии с требованиями. Защита производится после оформления отчета по работе.

Во время выполнения заданий в учебной аудитории обучающийся может консультироваться с преподавателем, определять наиболее эффективные методы решения поставленных задач. Если какая-то часть задания остается не выполненной, обучающийся может продолжить её выполнение во время внеаудиторной самостоятельной работы.

Для оценки полученных знаний и освоения учебного материала по каждому разделу и в целом по дисциплине преподаватель использует формы текущего, промежуточного и итогового контроля знаний обучающихся.

2. Методические рекомендации обучающимся

Приступая к изучению новой учебной дисциплины, обучающиеся должны ознакомиться с рабочей программой, оценочными материалами, учебной, научной и методической литературой, имеющейся в ЭИОС СКФ МТУСИ,

Глубина усвоения дисциплины зависит от активной и систематической работы обучающегося на лекциях и практических занятиях, а также в ходе самостоятельной работы, по изучению рекомендованной литературы.

2.1 Методические указания для обучающихся по лекционным занятиям

Важно сосредоточить внимание на содержании лекции. Это поможет лучше воспринимать учебный материал и уяснить взаимосвязь проблем по всей дисциплине.

Основное содержание лекции целесообразнее записывать в тетради в виде ключевых фраз, понятий, тезисов, обобщений, схем, опорных выводов. Необходимо обращать внимание на термины, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации. Желательно оставлять в конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющей материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

С целью уяснения теоретических положений, разрешения спорных ситуаций необходимо задавать преподавателю уточняющие вопросы. Для закрепления содержания лекции в памяти, необходимо во время самостоятельной работы внимательно прочесть свой конспект и дополнить его записями из учебников и рекомендованной литературы.

Конспектирование читаемых лекций и их последующая доработка способствует более глубокому усвоению знаний, и поэтому являются важной формой учебной деятельности обучающихся.

2.2 Методические указания для обучающихся по подготовке к практическим занятиям

Целью практических занятий является закрепление теоретических знаний, полученных при изучении дисциплины.

При подготовке к практическому занятию целесообразно выполнить следующие рекомендации:

- изучить основную литературу; ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях: журналах, газетах и т.д.;
- при необходимости доработать конспект лекций. При этом учесть рекомендации преподавателя и требования учебной программы.

При выполнении практических занятий основным методом обучения является самостоятельная работа обучающегося под управлением преподавателя. На них пополняются теоретические знания обучающихся, их умение творчески мыслить, анализировать, обобщать изученный материал, проверяется отношение обучающихся к будущей профессиональной деятельности.

Оценка выполненной работы осуществляется преподавателем комплексно: по результатам выполнения заданий, устному сообщению и оформлению работы.

После подведения итогов занятия обучающийся обязан устранить недостатки, отмеченные преподавателем при оценке его работы.

Для подготовки и выполнения практических занятий используется учебно-методическое пособие: *Введение в информационную безопасность: Учебное пособие для вузов / А.А. Малюк, В.И. Королев, В.М. Фомичев; Под ред. В.С. Горбатов. - Москва: Гор. линия-Телеком, 2011. - 288 с. URL: <https://znanium.ru/catalog/product/265558>. — Режим доступа: для авторизир. Пользователей.*

3. Методические рекомендации для обучающихся по самостоятельной работе

Самостоятельная работа обучающихся 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.

Самостоятельная работа во внеаудиторное время включает в себя:

- повторение лекционного материала;
- подготовки к лабораторным работам (практическим занятиям);
- изучения учебной и научной литературы;
- решения задач, выданных на практических занятиях;
- подготовки к тестированию;
- выделение наиболее сложных и проблемных вопросов по изучаемой теме, получение разъяснений и рекомендаций по данным вопросам с преподавателями кафедры на их еженедельных консультациях.
- проведение самоконтроля путем ответов на вопросы текущего контроля знаний, решения представленных в учебно-методических материалах кафедры задач, тестов, написания рефератов по отдельным вопросам изучаемой дисциплины.

Перед выполнением внеаудиторной самостоятельной работы преподаватель проводит инструктаж (консультацию) с определением цели задания, его содержания, сроков выполнения, основных требований к результатам работы, критериев оценки, форм контроля и перечня источников и литературы.

Обычно постановку задачи обучающимся на проведение самостоятельной работы преподаватель осуществляет на одном из занятий, предшествующему данному.

Методику самостоятельной работы все обучающиеся выбирают индивидуально.

Самостоятельная работа обучающихся над усвоением материала по дисциплине может выполняться в помещении для самостоятельной работы СКФ МТУСИ, посредством использования электронной библиотеки и ЭИОС.