

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


«28» 04

Н.А. Андреева

2026 г.

Рабочая программа дисциплины

Б1.О.35 Проектный практикум

Кафедра

Информационная безопасность

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/сем.
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	4	144/2
Контактная работа, в том числе (по семестрам, курсам):		72/2
Лекции		
Лабораторных работ		
Практических занятий		72/2
Семинаров		
Самостоятельная работа		72/2
Контроль		
Число контрольных работ (по курсам)		
Число КР (по семестрам, курсам)		
Число КП (по семестрам, курсам)		
Число зачетов с разбивкой по семестрам		1/2
Число экзаменов с разбивкой по семестрам (курсам)		

Программу составил:

К.т.н, доцент Маршаков Д.В.

Рабочая программа дисциплины
«Проектный практикум»

Разработана в соответствии с ФГОС ВО:

направления подготовки 10.03.01 «Информационная безопасность», утвержденным приказом Министерства науки и высшего образования Российской Федерации от 17 ноября 2020 г. N 1427

Составлена на основании учебных планов

направления 10.03.01 Информационная безопасность, профиль «Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)», одобренного Учёным советом СКФ МТУСИ, протокол № 8 от 31.03 2026, 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 "**Проектный практикум**" являются формирование у обучающихся знаний в области разработки, построения и контроля ИТ-инфраструктуры организации, моделирования компьютерных систем, навыков проверки их безопасности, мониторинга и устранения последствий инцидентов информационной безопасности.

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:

ОПК-12: Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	
Знать:	
- принципы построения и контроля ИТ-инфраструктуры виртуальной организации; - превентивные меры по предупреждению компьютерных атак и инцидентов.	
Уметь:	
- моделировать типовые и специализированные информационные системы; - активировать векторы компьютерных атак, характерные для внешнего и внутреннего нарушителей.	
Владеть:	
- навыками мониторинга событий информационной безопасности, расследования инцидентов информационной безопасности; - навыками выявления и нейтрализации компьютерных атак, оценки защищённости элементов информационных сетей.	

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.05 Введение в информационные технологии
2	Б1.В.06 Введение в профессию

4. Структура и содержание дисциплины

4.1. Очная форма обучения, 4 года (всего 144 часов, из них 72 часа аудиторных)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
1	2	3	4	5	6
Курс 1, Семестр 2					
Модуль 1: Основы проектирования компьютерных систем и сетей					
1.1	<u>Практическая работа 1. Проектирование и эксплуатация сетевой инфраструктуры организации</u> Основы построения и администрирования компьютерных сетей, адресация и маршрутизация в компьютерных сетях, программы и утилиты анализа трафика и удаленного доступа к компьютерным системам	Пр.	12	ОПК-12	Л1.1 Л1.3 Л2.1 Л2.2
1.2	Модель OSI и TCP/IP, топологии компьютерных сетей, протоколы передачи данных, сегментация сети, сетевые устройства, виртуализация сетей, функционал Wireshark, Tcpdump, Nmap, PuTTY	СРС	12	ОПК-12	Л1.1 Л1.3 Л2.1 Л2.2
1.3	<u>Практическая работа 2. Формирование документации на компьютерные системы и сети</u> Разработка технических заданий на создание систем и сетей, программной и эксплуатационной документации, изучение требований по обеспечению безопасности информации	Пр.	8	ОПК-12	Л1.1 Л1.3 Л2.2
1.4	Частные технические задания на создание системы защиты, виды конструкторской и эксплуатационной документации (руководства, инструкции), содержащей сведения о назначении и функциях, составе и архитектуре систем и сетей, о группах пользователей и уровне их полномочий и типах доступа, о внешних и внутренних интерфейсах	СРС	8	ОПК-12	Л1.1 Л1.3 Л2.2
1.5	<u>Практическая работа 3. Векторы удаленных компьютерных атак</u> Базовые схемы реализации угроз безопасности информации, реализуемых с использованием протоколов межсетевого взаимодействия, шаблоны компьютерных атак, содержащиеся в базах данных сети Интернет	Пр.	12	ОПК-12	Л1.1 Л1.2 Л2.1 Л2.2
1.6	Матрица MITRE ATT&CK, механизмы фишинговых атак, принципы построения атак на сетевую инфраструктуру, индикаторы векторов атак, моделирование векторов атак, принципы пентестинга	СРС	12	ОПК-12	Л1.1 Л1.2 Л2.1 Л2.2
Модуль 2: Разработка сценария киберучений					
2.1	<u>Практическая работа 4. Моделирование угроз безопасности компьютерных систем</u> Перечень угроз безопасности информации, банк угроз безопасности информации ФСТЭК России, оценка актуальности угроз с учетом архитектуры систем и сетей	Пр.	12	ОПК-12	Л1.1 Л1.2 Л1.3 Л2.2
2.2	Методика оценки угроз безопасности информации ФСТЭК России, базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных	СРС	12	ОПК-12	Л1.1 Л1.2 Л1.3 Л2.2
2.3	<u>Практическая работа 5. Конфигуратор сценариев кибератак программного комплекса «Ampire»</u> Назначение и состав ПК «Ampire», ролевая модель, построение процесса киберучений, создание и анализ	Пр.	12	ОПК-12	Л1.1 Л1.2 Л1.3 Л2.3

	карточек инцидентов ИБ, основы конфигурирования базовых сценариев кибератаки виртуальной сетевой инфраструктуры				
2.4	Изучение технической документация систем обнаружения вторжений и атак, программно-аппаратных комплексов VipNet IDS NS, VipNet TIAS, Security Onion	CPC	12	ОПК-12	Л1.1 Л1.2 Л1.3 Л2.3
2.5	<u>Практическая работа 6. Разработка сценария атаки и защиты ИТ-инфраструктуры предприятия</u> Разработка логической схемы корпоративной сети предприятия, проектирование модели Cyber kill chain, формирование легенды, разработка методических рекомендаций для пентестинга (Red Team), мониторинга и устранения инцидентов (Blue Team)	Пр.	16	ОПК-12	Л1.1 Л1.2 Л1.3 Л2.3
2.6	База знаний (угроз, уязвимостей и инцидентов) киберполигона Ampire, база данных уязвимостей CVE, стандарт OVAL, система классификации уязвимостей CWE, шаблоны компьютерных атак внутренних и внешних нарушителей, методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств ФСТЭК России	CPC	16	ОПК-12	Л1.1 Л1.2 Л2.2 Л2.3
	<u>Зачет</u>			ОПК-12	Л1.1 Л1.2 Л2.2 Л2.3
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.	Защита компьютерной информации. Эффективные методы и средства	Саратов: Профобразование, 2024.	Э1
Л1.2	Скрипник Д.А.	Обеспечение безопасности персональных данных: учебное пособие	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024.	Э2
Л1.3	Басан Е.С., Пескова О.Ю.	Безопасность сетей ЭВМ: учебное пособие	Ростов-на-Дону, Таганрог: Издательство Южного федерального университета, 2024.	Э3
5.1.2 Дополнительная литература				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л2.1	Брюхомицкий Ю.А.	Безопасность информационных технологий. В 2 частях. Ч.1: учебное пособие	Ростов-на-Дону, Таганрог: Издательство Южного федерального университета, 2020.	Э4
Л2.2	Башлы П.Н., Бабаш А.В., Баранова Е.К.	Информационная безопасность и защита информации: учебное пособие	Москва: Евразийский открытый институт, 2012.	Э5

Л2.3	Конев А.А., Якимук А.Ю.	Выявление инцидентов и противодействие атакам на объекты критической информационной инфраструктуры: учебно-методическое пособие	Томск: Томский государственный университет систем управления и радиоэлектроники, 2022.	Э6
------	----------------------------	---	--	----

5.1.3 Методическое обеспечение

Код	Авторы, составители	Заглавие	Издательство, год	Кол.
ЛЗ.1	Ванюшина А.В.	Практикум по дисциплине «Проектный практикум» направление подготовки 10.03.01 Информационная безопасность	Москва: МТУСИ, 2025	Э7

5.2 Электронные образовательные ресурсы

Э1	https://www.iprbookshop.ru/145909.html
Э2	https://www.iprbookshop.ru/133952.html
Э3	https://www.iprbookshop.ru/145108.html
Э4	https://www.iprbookshop.ru/107943.html
Э5	https://www.iprbookshop.ru/10677.html
Э6	https://www.iprbookshop.ru/152786.html
Э7	https://elib.mtuci.ru/view.php?book_id=34690

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	Электронный ресурс http://www.securitylab.ru/

5.4 Программное обеспечение

СКФ МТУСИ обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:

П.1	Linux (свободное ПО)
П.2	LibreOffice (свободное ПО)
П.3	Яндекс Браузер (свободное ПО)
П.4	Wireshark (свободное ПО)
П.5	PuTTY (свободное ПО)

6. Материально-техническое обеспечение дисциплины

6.1 МТО лекционных занятий

1	Лекционная аудитория, оснащенная проектором, ПК (ноутбуком), экраном
---	--

6.2 МТО лабораторных работ и практических занятий

1	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.О.35 Проектный практикум» 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 обучающимся, 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
ОПК-12		
Знать:		
- принципы построения и контроля ИТ-инфраструктуры виртуальной организации	Контрольная работа 1	Модуль 1 0–10 «Неудовлетворительно» - 0-1 «Неудовлетворительно» – 2 «Удовлетворительно» – 4 «Хорошо» – 7 «Отлично» – 10
- превентивные меры по предупреждению компьютерных атак и инцидентов.	Контрольная работа 2	Модуль 2 0–10 «Неудовлетворительно» - 0-1 «Неудовлетворительно» – 2 «Удовлетворительно» – 4 «Хорошо» – 7 «Отлично» – 10
Уметь:		
- моделировать типовые и специализированные информационные системы;	Практическая работа 1	Модуль 1 0–15 «Неудовлетворительно» - 0-1 «Неудовлетворительно» – 2 «Удовлетворительно» – 5 «Хорошо» – 10 «Отлично» – 15
	Практическая работа 2	Модуль 1 0–10 «Неудовлетворительно» - 0-1 «Неудовлетворительно» – 2 «Удовлетворительно» – 4 «Хорошо» – 7 «Отлично» – 10
- активировать векторы компьютерных атак, характерные для внешнего и внутреннего нарушителей	Практическая работа 6	Модуль 2 0–20 «Неудовлетворительно» - 0-1 «Неудовлетворительно» – 5 «Удовлетворительно» – 10 «Хорошо» – 15 «Отлично» – 20
Владеть:		
- навыками мониторинга событий информационной безопасности, расследования инцидентов информационной безопасности;	Практическая работа 3	Модуль 1 0–15 «Неудовлетворительно» - 0-1 «Неудовлетворительно» – 2-4 «Удовлетворительно» – 5-7 «Хорошо» – 8-10 «Отлично» – 11-15

	Практическая работа 4	Модуль 2 0–10 «Неудовлетворительно» – 0-3 «Удовлетворительно» – 4-5 «Хорошо» – 6-7 «Отлично» – 8-10
- навыками выявления и нейтрализации компьютерных атак, оценки защищённости элементов информационных сетей.	Практическая работа 5	Модуль 2 0–10 «Неудовлетворительно» – 0-2 «Удовлетворительно» – 3-5 «Хорошо» – 6-7 «Отлично» – 8-10
	Зачет	0-100 «Не зачтено» – 0-40 «Зачтено» – 41-100

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 3 практических занятия. Знание материала оценивается по контрольной работе, состоящей из двух вопросов, максимальное количество баллов за контрольную работу составляет 10, умения и навыки по результатам защиты практических работ, в ходе которых обучающийся получает максимум 40 баллов. Общее максимальное количество баллов за модуль 1 составляет 50.

Вопросы для контрольной работы 1 (ОПК-12):

1. Перечислите и кратко охарактеризуйте уровни модели OSI. Приведите отличия модели OSI от стека протоколов TCP/IP.
2. Принцип маршрутизации в компьютерных сетях.
3. Принцип сетевой адресации. Основные различия IPv4 и IPv6.
4. Основные топологии компьютерных сетей.
5. Цели и методы сегментации компьютерной сети.
6. Функционал и сценарии применения Wireshark, Tcpdump, Nmap. Примеры команд для сканирования портов, определения ОС удалённого хоста, обнаружения активных узлов в сети.
7. Технологии виртуализации компьютерных сетей.
8. Разделы технического задания при проектировании корпоративной сети.
9. Виды эксплуатационной документации для проектируемой ИТ-системы.
10. Базовые схемы реализации сетевых атак с использованием протоколов межсетевого взаимодействия.
11. Матрица MITRE ATT&CK и её применение в кибербезопасности.
12. Типовые индикаторы компрометации для фишинговой атаки.
13. Основные этапы тестирования на проникновение. Роль команд Red Team и Blue Team на каждом этапе.
14. Пример шаблона компьютерной атаки из открытых баз данных: уязвимость, вектор атаки, ПО для эксплуатации и рекомендуемые меры защиты.

Практическое занятие №1. Проектирование и эксплуатация сетевой инфраструктуры организации.

Контрольные вопросы (ОПК-12):

1. Основные этапы проектирования сетевой инфраструктуры организации.
2. Принцип адресации в компьютерных сетях. Разница между частными и публичными IP-адресами.
3. Принцип работы маршрутизации в компьютерных сетях. Что такое таблица маршрутизации и какие основные поля она содержит?
4. Краткая характеристика утилит, которые используются для анализа сетевого трафика и диагностики соединений.
5. Перечислите основные протоколы удалённого доступа к компьютерным системам. Какие из них обеспечивают шифрование передаваемых данных?
6. Что такое подсеть и для чего она используется в корпоративной сети? Приведите пример: разделите сеть 192.168.1.0/24 на 4 подсети с равным числом адресов.

Практическое занятие №2. Формирование документации на компьютерные системы и сети.

Контрольные вопросы (ОПК-12):

1. Ключевые разделы технического задания на создание компьютерной системы или сети.
2. Основные виды эксплуатационной документации для компьютерных систем и сетей.
3. Структура и содержание руководства пользователя для сетевого оборудования. Перечислите примеры разделов и кратко поясните, какая информация в них должна быть представлена.
4. Какие требования к обеспечению безопасности информации должны быть отражены в документации на компьютерную систему или сеть?
5. Различие между программной и эксплуатационной документацией. Примеры документов каждого типа.
6. Опишите процесс оформления, согласования и утверждения технической документации на компьютерные системы и сети.

Практическое занятие №3. Векторы удаленных компьютерных атак.

Контрольные вопросы (ОПК-12):

1. Что такое вектор компьютерной атаки? Назовите ключевые компоненты вектора удалённой атаки.
2. Перечислите основные этапы реализации удалённой атаки через сетевые протоколы.
3. Что понимается под «шаблоном компьютерной атаки»?
4. Перечислите известные схемы реализации угроз безопасности информации, реализуемые с использованием протоколов межсетевого взаимодействия.
5. Приведите пример атаки на протокол TCP: какая уязвимость используется и какой метод защиты эффективен против неё?
6. Сравните DNS spoofing и MITM через ARP-подмену по следующим параметрам: уровень модели OSI, одно условие для реализации, способ обнаружения.

Модуль 2 (50 баллов):

Модуль содержит 3 практических занятия. Знание материала оценивается по контрольной работе, состоящей из двух вопросов, максимальное количество баллов за контрольную работу составляет 10, умения и навыки по результатам защиты практических работ, в ходе которых обучающийся получает максимум 40 баллов. Общее максимальное количество баллов за модуль 2 составляет 50.

Вопросы для контрольной работы 2 (ОПК-12):

1. Значение, содержание и целевое применение банка угроз безопасности информации ФСТЭК России.
2. Ключевые параметры, учитываемые при оценке актуальности угроз с учётом архитектуры систем и сетей.
3. Сущность методики оценки угроз безопасности информации ФСТЭК России.
4. Основные положения базовой модели угроз безопасности персональных данных в ИСПДн.
5. Ключевые функциональные модули ПК «Ampire».
6. Суть ролевой модели в контексте киберучений.
7. Основные элементы, включаемые в карточку инцидента ИБ.
8. Отличительные особенности программно-аппаратных комплексов VipNet IDS NS и VipNet TIAS.
9. Ключевые этапы проектирования логической схемы корпоративной сети предприятия.
10. Сущность модели Cyber kill chain и область её применения.
11. Отличительные особенности работы Red Team от Blue Team в контексте кибербезопасности.
12. Содержание базы знаний киберполигона «Ampire».
13. Различия между базами CVE и CWE.
14. Стандарт OVAL и область его применения.
15. Критерии оценки уровня критичности уязвимостей согласно методике ФСТЭК России?

Практическое занятие №4. Моделирование угроз безопасности компьютерных систем.

Контрольные вопросы (ОПК-12):

1. Что входит в перечень типовых угроз безопасности информации?
2. Какие ключевые параметры учитывает оценка актуальности угроз?
3. Как архитектура ИС влияет на набор актуальных угроз?
4. Каковы этапы моделирования угроз по методике ФСТЭК России?
5. Как соотносятся уязвимости и угрозы в модели угроз?
6. Какие исходные данные нужны для оценки актуальности угрозы?

Практическое занятие №5. Конфигуратор сценариев кибератак программного комплекса «Ampire».

Контрольные вопросы (ОПК-12):

1. Для чего предназначен программный комплекс (ПК) «Ampire»?
2. Какие основные компоненты входят в состав ПК «Ampire»?
3. В чём суть ролевой модели в рамках киберучений на «Ampire»?
4. Перечислите ключевые этапы построения процесса киберучений в «Ampire».
5. Что представляют собой карточки инцидентов ИБ и для чего они анализируются?
6. Какие базовые сценарии кибератак можно сконфигурировать в виртуальной сетевой инфраструктуре «Ampire»?

Практическое занятие №6. Разработка сценария атаки и защиты IT-инфраструктуры предприятия.

Контрольные вопросы (ОПК-12):

1. Какие ключевые элементы включают в себя логическая схема корпоративной сети предприятия?
2. Перечислите основные этапы модели Cyber kill chain.
3. Что понимается под «легендой» в контексте киберучений и для чего она формируется?
4. Каковы основные задачи команды Red Team при проведении пентестинга?
5. Назовите методические рекомендации для команды Blue Team по мониторингу и устранению инцидентов ИБ.
6. Как взаимосвязаны разработка сценария атаки и меры защиты IT-инфраструктуры в рамках киберучений?

По результатам практического занятия представляется проект на тему: «**Сценарий проведения киберучений на базе программного комплекса Ampire**». Название проекта формируется обучающимися индивидуально, исходя из заданной им IT-инфраструктуры организации, выбранных объектов атаки, сценария кибератаки и мер противодействия.

Примерная структура проекта:

Название сценария
Цель сценария <i>Утверждение, воплощающее в себе общий результат, которого хотели бы достичь.</i>
Проектирование IT-инфраструктуры <i>Описание IT-инфраструктуры организации, составление логической схемы сценария, технического задания и эксплуатационной документации</i>
Легенда <i>Описание типа нарушителя, его мотивации, квалификации, основных этапов компьютерной атаки, целевых информационных активов</i>
Сценарий проникновения (кибератаки) <i>Краткая характеристика реализуемых угроз и уязвимостей, представление модели Cyber kill chain, описание применяемых инструментов удаленного доступа, процесса сбора информации, вторжения в операционную среду, реализации несанкционированных действий, ликвидации следов атаки</i>
Сценарий мониторинга <i>Описание способов детектирования определенных этапов выполнения сценария кибератаки, рекомендации составления карточек инцидентов ИБ с указанием идентификаторов уязвимостей и способов их устранения</i>
Сценарий реагирования <i>Описание способов устранения последствий инцидента, устранения уязвимостей, применения средств повышения кибербезопасности</i>
Роли и компетенции <i>Перечисление ролей в команде участников (пентестер (нарушитель), члены группы мониторинга, лидер группы реагирования, члены группы реагирования) и соответствующие им компетенции.</i>

1.3.2 Вопросы, выносимые на зачет по дисциплине (ОПК-12) (промежуточная аттестация):

1. Перечислите и кратко охарактеризуйте уровни модели OSI. Приведите отличия модели OSI от стека протоколов TCP/IP.
2. Принцип маршрутизации в компьютерных сетях.
3. Принцип сетевой адресации. Основные различия IPv4 и IPv6.
4. Основные топологии компьютерных сетей.
5. Цели и методы сегментации компьютерной сети.
6. Функционал и сценарии применения Wireshark, Tcpdump, Nmap. Примеры команд для сканирования портов, определения ОС удалённого хоста, обнаружения активных узлов в сети.
7. Технологии виртуализации компьютерных сетей.
8. Разделы технического задания при проектировании корпоративной сети.
9. Виды эксплуатационной документации для проектируемой ИТ-системы.
10. Базовые схемы реализации сетевых атак с использованием протоколов межсетевого взаимодействия.
11. Матрица MITRE ATT&CK и её применение в кибербезопасности.
12. Типовые индикаторы компрометации для фишинговой атаки.
13. Основные этапы тестирования на проникновение. Роль команд Red Team и Blue Team на каждом этапе.
14. Пример шаблона компьютерной атаки из открытых баз данных: уязвимость, вектор атаки, ПО для эксплуатации и рекомендуемые меры защиты.
15. Значение, содержание и целевое применение банка угроз безопасности информации ФСТЭК России.
16. Ключевые параметры, учитываемые при оценке актуальности угроз с учётом архитектуры систем и сетей.
17. Сущность методики оценки угроз безопасности информации ФСТЭК России.
18. Основные положения базовой модели угроз безопасности персональных данных в ИСПДн.
19. Ключевые функциональные модули ПК «Ampire».
20. Суть ролевой модели в контексте киберучений.
21. Основные элементы, включаемые в карточку инцидента ИБ.
22. Отличительные особенности программно-аппаратных комплексов VipNet IDS NS и VipNet TIAS.
23. Ключевые этапы проектирования логической схемы корпоративной сети предприятия.
24. Сущность модели Cyber kill chain и область её применения.
25. Отличительные особенности работы Red Team от Blue Team в контексте кибербезопасности.
26. Содержание базы знаний киберполигона «Ampire».
27. Различия между базами CVE и CWE.
28. Стандарт OVAL и область его применения.
29. Критерии оценки уровня критичности уязвимостей согласно методике ФСТЭК России?

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, представление индивидуального или группового проекта;
- промежуточная аттестация по дисциплине – в форме зачета.

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

- 1-й этап: допуск к выполнению практической работы – устный опрос с целью контроля знаний обучающихся теоретической части лабораторной работы и готовности к выполнению практических исследований;

- 2-й этап выполняется по окончании каждой практического занятия в форме индивидуального собеседования по выполненным исследованиям.

Контрольные работы выполняются в виде короткого устного ответа на один вопрос, изученный на предыдущем занятии в начале каждого последующего занятия.

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 баллы в рамках текущего контроля переводятся в оценку на зачете в соответствии со следующей шкалой:

- «не зачтено» - от 0 до 40 от максимального количества баллов;
- «зачтено» - от 41 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 (Распределение баллов по занятиям)
Модуль 1	50	10	40
Модуль 2	50	10	40
Зачет	100	100	

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

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

3. Промежуточная аттестация

Промежуточная аттестация проводится в форме зачета. Зачет проводится по расписанию в устном виде по билетам к зачету. Результаты аттестации заносятся в ведомость и зачетную книжку обучающегося.

Образец билета к зачету

	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 И.о.зав. кафедрой «ИБ» _____ А.Г.Жуковский « ____ » _____ 20 ____ г.
Направление подготовки: 10.03.01 Информационная безопасность Курсы: 1 Дисциплина: Проектный практикум		
Билет №1 1. Базовые схемы реализации сетевых атак с использованием протоколов межсетевого взаимодействия. 2. Ключевые этапы проектирования логической схемы корпоративной сети предприятия. к.т.н, доцент _____ Маршаков Д.В. « ____ » _____ 20 ____ г.		

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

4. ТЕСТОВЫЕ ЗАДАНИЯ ПО ДИСЦИПЛИНЕ (ОПК-12)

Тестовые задания позволяют оценить уровень сформированности компетенции ОПК-12.

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.

ОПК-12. Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений.

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.О.35 Проектный практикум	Организация процесса отражения атаки в проектируемом сценарии киберучения происходит с участием команд: 1. Мониторинга 2. Реагирования 3. Расследования 4. Оценивания
2	Б1.О.35 Проектный практикум	Задачей команды «Blue Team» в отношении к спроектированной компьютерной системе является: 1. Защита системы от реальных кибератак 2. Тестирование системы на проникновение 3. Разработка и внедрение мер по повышению уровня защиты информации системы
3	Б1.О.35 Проектный практикум	Задачей команды «Red Team» в отношении к спроектированной компьютерной системе является: 1. Защита системы от реальных кибератак 2. Тестирование системы на проникновение 3. Разработка и внедрение мер по повышению уровня защиты информации системы
4	Б1.О.35 Проектный практикум	Нежелательное событие, нарушившее безопасность информации это: 1. Инцидент 2. Уязвимость 3. Угроза 4. Риск
5	Б1.О.35 Проектный практикум	Последовательность действий, использующих уязвимости информационной системы и приводящих к нарушению политики безопасности: 1. Кибератака 2. Угроза 3. Риск 4. Инцидент
6	Б1.О.35 Проектный практикум	При проектировании сети 185.88.181.0/24 маской узла с адресом 185.88.181.5 является: 1. 255.255.255.0 2. 255.255.240.0 3. 255.255.255.255

№	Дисциплина	Тексты заданий
		4. 255.240.0.0
7	Б1.О.35 Проектный практикум	Атака Brute-force на компьютерную систему проводится с целью: 1. Удаленного выполнения кода в программном обеспечении CMS 2. Туннелирования ТСП-соединений 3. Перебора всех возможных вариантов пароля 4. Выполнения произвольного запроса к базе данных
8	Б1.О.35 Проектный практикум	К категории секретной информации относятся: 1. Государственная тайна 2. Персональные данные 3. Коммерческая тайна 4. Профессиональная тайна 5. Все перечисленное
9	Б1.О.35 Проектный практикум	К категории конфиденциальной информации относится: 1. Государственная тайна 2. Персональные данные 3. Коммерческая тайна 4. Профессиональная тайна 5. Все перечисленное
10	Б1.О.35 Проектный практикум	Средство защиты информации для автоматизации мониторинга событий, протекающих в компьютерной системе или сети, а также анализа этих события в поисках признаков инцидента информационной безопасности: 1. Система обнаружения вторжений 2. Межсетевой экран 3. Антивирусное ПО 4. Система разграничения доступа

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

№	Дисциплина	Тексты заданий
11	Б1.О.35 Проектный практикум	Укажите соответствие объектов при проектировании шаблона «Предприятие» в системе Ampire: 1. Сегмент сети Интернет 2. Сегмент корпоративного центра обработки данных 3. Сегмент пользовательского отдела 4. Сегмент АСУ ТП А. Прямоугольник на схеме «Интернет» Б. Прямоугольник на схеме «Data Center» В. Прямоугольник на схеме «Office Users» Г. Прямоугольник на схеме «ASU»
12	Б1.О.35 Проектный практикум	Укажите соответствие функционала средств обнаружения вторжений, применяемых в системе Ampire: 1. Автоматическое обнаружение угроз и регистрация событий в журнале 2. Интеллектуальный анализ угроз безопасности информации, относящихся к атакам 3. Мониторинг безопасности, обнаружение инцидентов и анализ сетевого трафика А. ViPNet IDS NS Б. ViPNet TIAS В. SecOnion
13	Б1.О.35 Проектный практикум	Установите соответствие между названием топологии проектируемой компьютерной сети и её описанием: 1. Каждый компьютер подключается непосредственно к общему центральному устройству 2. Данные передаются по замкнутой траектории последовательно от одного компьютера к другому 3. Используется один кабель, к которому подключены все компьютеры сети 4. Каждый компьютер непосредственно связан со всеми остальными А. Звезда Б. Кольцо В. Общая шина Г. Полносвязная

14	Б1.О.35 Проектный практикум	Укажите соответствие между приведенными объектами информатизации: 1. Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств 2. Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций 3. Технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники 4. Система, функционирующая без участия человека А. Информационная система Б. Автоматизированная система В. Информационно-телекоммуникационная сеть Г. Автоматическая система
----	-----------------------------------	---

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

Инструкция: Прочитайте текст и установите правильную последовательность

№	Дисциплина	Тексты заданий
15	Б1.О.35 Проектный практикум	Восстановите логическую цепочку, по которой целесообразно проводить анализ актуальности угроз безопасности: 1. Источник угрозы 2. Уязвимость 3. Угроза 4. Атака
16	Б1.О.35 Проектный практикум	Укажите правильную последовательность обработки инцидента информационной безопасности: 1. Обнаружение инцидента 2. Создание карточки инцидента 3. Реагирование на инцидент 4. Расследование инцидента
17	Б1.О.35 Проектный практикум	Расставьте в порядке возрастания уровней грифы секретности для носителей сведений, составляющих государственную тайну: 1. Секретно 2. Совершенно секретно 3. Особой важности

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

Инструкция: Прочитайте текст и запишите обоснованный ответ

№	Дисциплина	Тексты заданий
18	Б1.О.35 Проектный практикум	Впишите пропущенное слово. Слабость одного или нескольких активов, которая может быть использована одной или несколькими угрозами - это _____.
19	Б1.О.35 Проектный практикум	Впишите пропущенное слово. Потенциальная причина нежелательного инцидента, который может причинить вред системе или организации это _____.
20	Б1.О.35 Проектный практикум	Впишите пропущенное слово. Лицо, предпринявшее попытку выполнения запрещенных действий по ошибке, незнанию или осознанно со злым умыслом или без такового называется _____.

Система оценивания выполнения тестовых заданий по компетенции ОПК-12

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.

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

Каждое практическое занятие должна быть защищено в соответствии с требованиями. Защита производится после оформления отчета по практической 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 практических занятиях, а также в ходе самостоятельной работы, по изучению рекомендованной литературы.

2.1 Методические указания для обучающихся по подготовке к практическим занятиям

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: *Ванюшина А.В. Практикум по дисциплине «Проектный практикум» направления подготовки 10.03.01 Информационная безопасность*, URL: https://elibr.mtuci.ru/view.php?book_id=34690 (дата обращения: 30.04.2025). — 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:

- подготовки к 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.

Самостоятельная работа обучающихся направлена на углубленное изучение разделов и тем рабочей программы и предполагает изучение рекомендуемых литературных источников, выполнение домашних заданий и проведение исследований разного характера. Работа основывается на анализе литературных источников и материалов, публикуемых в Интернете, а также реальных речевых и языковых фактов, личных наблюдений. Также самостоятельная работа включает подготовку и анализ материалов по темам пропущенных занятий.

Самостоятельная работа по дисциплине включает следующие виды деятельности:

- поиск (подбор) и обзор литературы, электронных источников информации по индивидуально заданной проблеме курса, написание доклада, проектной работы по заданной проблеме;
- выполнение задания по пропущенной или плохо усвоенной теме;
- самостоятельный поиск информации в Интернете и других источниках;
- изучение материала, вынесенного на самостоятельную проработку (отдельные темы, параграфы);
- выполнение в лаборатории самостоятельных исследований с использованием программно-аппаратного комплекса и моделирующих программ;
- подготовка к практическим занятиям;
- подготовка к зачету. 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, предшествующем 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.