

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.О.29

Методы и средства криптографической защиты информации

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 (очная форма обучения (ОФО))

Вид учебной работы	ОФ	
	ЗЕ	часов
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	5	180/6
Контактная работа, в том числе (по семестрам, курсам):		80/6
Лекции		32/6
Лабораторных работ		32/6
Практических занятий		16/6
Семинаров		
Самостоятельная работа		64/6
Контроль		36/6
Число контрольных работ (по курсам)		
Число КР (по семестрам, курсам)		1/6
Число КП (по семестрам, курсам)		
Число зачетов с разбивкой по семестрам (курсам)		
Число экзаменов с разбивкой по семестрам (курсам)		1/6

Программу составили:

К.т.н., доцент Шухардин А.Н.

Рабочая программа дисциплины

Методы и средства криптографической защиты информации

Разработана в соответствии с ФГОС ВО

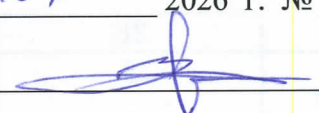
направление подготовки 10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ,
утвержденное приказом Министерства науки и высшего образования Российской
Федерации от 17 ноября 2020 г. № 1427.

Составлена на основании учебного плана

направления 10.03.01 «Информационная безопасность» профиля «Безопасность ком-
пьютерных систем(по отрасли или в сфере профессиональной деятельности)», одоб-
ренного Учёным советом СКФ МТУСИ, протокол № 8 от 31.03 2026г, и
утвержденного директором СКФ МТУСИ 31.03 2026 г.

Одобрена на заседании кафедры
«Информационная безопасность»

Протокол от 28.04 2026 г. № 9

И.О.Зав. кафедрой  Жуковский А.Г.

1. Цели изучения дисциплины

Целью преподавания дисциплины является формирование у обучаемых знаний в области криптографических методов защиты информации, типовых программно-аппаратных средств криптографической защиты информации и инфокоммуникаций от несанкционированного доступа.

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-6: Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
Знать (Необходимые знания):
- нормативные и правовые акты, регулирующие деятельность по обеспечению защиты информации от утечки и несанкционированных действий; - требования нормативных правовых актов и нормативных методических документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю при организации защиты информации ограниченного доступа в компьютерных сетях.
Уметь (Необходимые умения):
- определять ресурсы, необходимые для обеспечения безопасности автоматизированных систем; - осуществлять подбор средств, соответствующих требованиям нормативных правовых актов и нормативных методических документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю, при организации защиты информации ограниченного доступа в компьютерных сетях.
Владеть (Трудовые действия):
- навыками анализа требований по защите средств вычислительной техники и автоматизированных систем на основе показателей защищенности; - навыками организации защиты информации ограниченного доступа в компьютерных сетях, соответствующей требованиям нормативных правовых актов и нормативных методических документов.
ОПК-9: Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности
Знать (Необходимые знания):
- принципы использования средств криптографической защиты информации при решении задач профессиональной деятельности; - методики использования технических средств защиты информации для решения практических задач обеспечения информационной безопасности.
Уметь (Необходимые умения):
- использовать программно-аппаратные средства криптографической защиты информации для решения практических задач; - решать задачи защиты информации от утечки по техническим каналам, сетей и систем передачи информации.
Владеть (Трудовые действия):
- навыками установки и настройки программно-аппаратных средств криптографической защиты

информации для решения практических задач;
 - навыками использования специальных технических средств при защите информации от утечки по техническим каналам, сетей и систем передачи информации.

3. Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Б1.О.27 «Основы информационной безопасности»
2	Б1.О.05 «Введение в информационные технологии»
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Б1.В.02 Комплексное обеспечение защиты информации объекта
2	Б1.О.36.02 «Криптографические протоколы» Б1.О.36.03 «Безопасность компьютерных сетей»

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 180 часов, 80 часов контактной работы)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
Курс 3, Семестр 6					
Модуль 1 Криптографические методы защиты информации – 54 (46+8) часов					
1.1	Лекция 1 Основные задачи современной криптографии. Конфиденциальность. Целостность. Аутентификация. Неотслеживаемость. Цифровая подпись. Управление ключами. Общие требования к криптосистемам.	Лек	2	ОПК-6,	Л1.1 Л1.2 Л1.3
1.2	Лекция 2. Классификация шифров. Математические модели шифров. Математические модели открытого текста. Критерии распознавания открытого текста.	Лек.	2	ОПК-6,	Л1.1 Л1.2 Л1.3
1.3	Лекция 3. Шифры перестановки. Шифр Сцигала. Маршрутные перестановки. Шифры вертикальной перестановки. Поворотные решетки. Задача Эйлера. Элементы криптоанализа шифров перестановки.	Лек	2	ОПК-6,	Л1.1 Л1.2 Л1.3
1.4	Лекция 4. Шифры замены. Поточные шифры простой замены. Шифры многоалфавитной замены. Биграммные и n-граммные шифры замены. Матричные шифры. Модель шифров замены. Классификация шифров замены. Криптоанализ поточного шифра простой замены.	Лек	2	ОПК-6,	Л1.1 Л1.2 Л1.3
1.5	Лекция 5. Шифры гаммирования. Основные требования к гамме. Шифр Виженера. Одноразовый блокнот К.Шеннона. Аддитивные методы шифрования. Режим гаммирования ГОСТ 28147-89 и Магма.	Лек	2	ОПК-6,	Л1.1 Л1.2 Л1.3
1.6	Лекция 6. Поточные системы шифрования. Регистры сдвига с обратной связью. Скремблеры. Методы рандомизации сообщений. Поточные шифрсистемы.	Лек	2	ОПК-6,	Л1.1 Л1.2 Л1.3
1.7	Лекция 7. Блочные системы шифрования. Блочные системы шифрования. Конструкции Фейстеля. Режимы	Лек	2	ОПК-6,	Л1.1 Л1.2

	шифрования блочных шифров. Алгоритмы блочного шифрования.				Л1.3
1.8	Лекция 8. Системы шифрования с открытыми ключами. Асимметричные системы. Открытое распределение ключей. Схема Диффи-Хеллмана. Криптосистема RSA. Схема шифрования Эль-Гамала. Криптография на эллиптических кривых. Криптоанализ шифра RSA.	Лек	2	ОПК-6,	Л1.1 Л1.2 Л1.3
1.9	Лекция 9 Электронные цифровые подписи. Механизм действия электронной цифровой подписи. Функции хэширования. Алгоритмы цифровой подписи. Криптоанализ односторонних хэш-функций.	Лек	2	ОПК-6,	Л1.1 Л1.2 Л1.3
1.10	Практическое занятие №1 Криптоанализ и дешифрование. Правило Керкхоффа. Криптография и теория чисел.	ПЗ	4	ОПК-6	Л3.1
1.11	Практическое занятие №2. Операторы шифрования: общие свойства и требования. Совершенная секретность и случайные ключи. Совершенный шифр Вернама. Информационная цена криптозащиты. Избыточность сообщений и её роль в криптоанализе. Оценка расстояния единственности.	ПЗ	4	ОПК-6,	Л3.1
1.12	Лабораторная работа №1. Моно и много алфавитные подстановки. Перестановки. Простейшие алгоритмы шифрования и расшифрования. Шифры Цезаря, Виженера. Криптоанализ или атака на шифры Цезаря и Виженера. Шифры на основе подстановки на алфавите и перестановки.	ЛР	4	ОПК-6,	Л3.2
1.13	Лабораторная работа № 2 Принципы блочного многоаундового шифрования. Схема Фейстеля. Генерирование блочных шифров.	ЛР	4	ОПК-6	Л3.2
1.14	Лабораторная работа № 3 Принципы блочного многоаундового шифрования. Блочный шифр DES, разновидности алгоритма DES.	ЛР	4	ОПК-6	Л3.2
1.15	Лабораторная работа № 4 Стандарты на электронную (цифровую) подпись: цифровая подпись DSS, цифровая подпись ГОСТ Р34.10-94. Цифровые подписи, основанные на симметричных криптосистемах.	ЛР	4	ОПК-6	Л3.2
1.16	Лабораторная работа № 5 «Анализ электронной цифровой подписи на основе криптосистемы Эль Гамала».	ЛР	4	ОПК-6	Л3.2
1.17	История появления шифров Основные этапы жизненного цикла вирусов; объекты внедрения, режимы функционирования и специальные функции вирусов Схемы заражения файлов; схемы заражения загрузчиков; способы маркировки, используемые вирусами	СРС	8	ОПК-6	Л1.1 Л1.2 Л1.3 Л2.1
Модуль 2 Средства криптографической защиты информации – 54 (34+20) часов					
2.1	Лекция 13. Нормативно-правовые основы криптографической защиты информации. Действующие стандарты криптографической защиты информации. Федеральный закон об электронной подписи. Нормативно-правовые акты ФСБ по обеспечению безопасности персональных данных с использованием СКЗИ. Нормативно-правовые акты ФСБ по обеспечению функционирования и эксплуатации СКЗИ. Виды работ и услуг, составляющих лицен-	Лек	4	ОПК-9	Л1.1 Л1.2 Л1.3

	зируемую деятельность с использованием СКЗИ. Порядок лицензирования деятельности с использованием СКЗИ. Правила сертификации СКЗИ по требованиям ФСБ.				
2.2	Лекция 14. Классификация средств криптографической защиты информации. Требования к средствам криптографической защиты информации. Программные СКЗИ. Особенности и примеры. Аппаратные и программно-аппаратные СКЗИ. Критерии выбора СКЗИ. Основные принципы построения СКЗИ. Принципы построения аппаратных СКЗИ. Принципы построения программных и программно-аппаратных СКЗИ. Основные подходы к обеспечению надежности СКЗИ	Лек	4	ОПК-9	Л1.1 Л1.2 Л1.3
2.3	Лекция 15. Средства криптографической защиты информации на персональном компьютере. Задачи обеспечения информационной безопасности на персональном компьютере с использованием СКЗИ. Криптографическая защита жестких дисков и съемных носителей. Средства шифрования, встроенные в операционную систему Windows. Шифрование архиваторов. СКЗИ свободного доступа. СКЗИ от несанкционированного доступа.	Лек	2	ОПК-9	Л1.1 Л1.2 Л1.3
2.4	Лекция 16. Средства криптографической защиты сетевого взаимодействия. Криптографические средства создания защищенных виртуальных сетей (VPN). Технология построения криптозащищенных туннелей. Криптографическая защита удаленного доступа к локальной сети. СКЗИ для передачи данных в локальных сетях. Сетевые протоколы криптографической защиты. Персональные криптографические средства аутентификации.	Лек	4	ОПК-9	Л1.1 Л1.2 Л1.3
2.6	Практическое занятие №3. Изучение разрешений ntfs и разрешений на общий ресурс в операционной системе	ПЗ	4	ОПК-9	Л3.1
2.7	Практическое занятие №4 Изучение аудита в операционной системе	ПЗ	4	ОПК-9	Л3.1
2.8	Лабораторная работа № 6 «Анализ электронной цифровой подписи на основе криптосистемы Эль Гамала».	ЛР	4	ОПК-9	Л3.2
	Лабораторная работа №7 Настройка шифрования и подписи документов в операционной системе	ЛР	4	ОПК-9	Л3.2
2.9	Лабораторная работа №8 Настройка VPN туннеля	ЛР	4	ОПК-9	Л3.2
2.10	Анализ структуры и принципов функционирования вычислительных сетей с позиции обеспечения информационной безопасности Угрозы информационно-программному обеспечению, характерные только для распределённой вычислительной среды Использование криптографических методов для защиты данных, циркулирующих в вычислительной сети	СРС	20	ОПК-9	Л1.1 Л1.2 Л1.3 Л2.1
Модуль 1 – Курсовое проектирование – 36 ч.					
3.1	Криптоанализ шифра Виженера	СРС	36	ОПК-6, ОПК-9	Л3.3
	Экзамен		36	ОПК-6, ОПК-9	Л1.1 Л1.2

					Л1.3 Л2.1 Л3.1 Л3.2 Л3.3
Итого – 180 часов					

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Рекомендуемая литература				
5.1.1. Основная литература				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л1.1	Ермакова, А. Ю. В. В. Лебедев	Методы и средства криптографической защиты информации : учебное пособие	М.: — Москва : РТУ МИРЭА, 2024. — 230 с.	Э1
Л1.2	Н. Н. Ушкова, А. А. Аксенова, М. Н. Нечаева [и др.]	Методы и средства криптографической защиты информации : учебное пособие	М. : РТУ МИРЭА, 2024. — 133 с.	Э2
Л1.3	Зайцев А.П., Мещеряков Р.Е., Шелупанов А.А.	Технические средства и методы защиты информации. Учебник для вузов. 7-е изд., перераб. и доп. - 2024	М.: Гор. линия-Телеком, 2024.	Э3
5.1.2. Дополнительная литература				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л2.1	Котов, Ю. А.	Котов, Ю. А. Криптографические методы защиты информации. Шифры : учебное пособие	Новосибирск : Новосибирский государственный технический университет, 2016. — 59 с.	Э4
5.1.3. Учебно-методическое обеспечение				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л3.1	Шухардин А.Н., Юхнов В.И.	Методические указания по проведению практических занятий по дисциплине «Методы и средства криптографической защиты информации».	РнД: СКФ МТУСИ, 2025. — 27 с.	Э5
Л3.2	Шухардин А.Н., Юхнов В.И.	Методические указания по проведению лабораторных работ по дисциплине «Методы и средства криптографической защиты информации».	РнД: СКФ МТУСИ, 2025. — 73 с.	Э6
Л3.3	Шухардин А.Н., Юхнов В.И.	Методические указания по выполнению курсовой работы по дисциплине «Методы и средства криптографической защиты информации»	РнД: СКФ МТУСИ, 2025. — 53 с.	Э7
5.2. Электронные образовательные ресурсы				
Э1	https://e.lanbook.com/book/420980			

Э2	https://e.lanbook.com/book/421076
Э3	https://elib.mtuci.ru/view.php?book_id=4112
Э4	https://www.iprbookshop.ru/91377.html
Э5	https://elib.mtuci.ru/view.php?book_id=170088
Э6	https://elib.mtuci.ru/view.php?book_id=170087
Э7	https://elib.mtuci.ru/view.php?book_id=170089

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

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

П.1	Kaspersky Endpoint Security
П.2	Операционная система Linux
П.3	MS Office
П.4	Oracle VM Virtual Box

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	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 (полнота, 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 «Методы и средства криптографической защиты информации Б1.О.29» для использования в 20___/20___ учебном году

Утверждаю

Зам. директора по УВР _____
«___» _____ 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-6: Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю		
Знать:		
- нормативные и правовые акты, регулирующие деятельность по обеспечению защиты информации от утечки и несанкционированных действий; - требования нормативных правовых актов и нормативных методических документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю при организации защиты информации ограниченного доступа в компьютерных сетях.	Контрольная работа	Модуль 1 0÷15 «Неудовлетворительно» - 0-5 «Удовлетворительно» - 6-9 «Хорошо» - 9-12 «Отлично» - 12-15
Уметь:		
- определять ресурсы, необходимые для обеспечения безопасности автоматизированных систем; - осуществлять подбор средств, соответствующих требованиям нормативных правовых актов и нормативных методических документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю, при организации защиты информации ограниченного доступа в компьютерных сетях.	Практическое занятие 1	Модуль 1 0÷5 «Неудовлетворительно» - 0-1 «Удовлетворительно» - 2-3 «Хорошо» - 3-4 «Отлично» - 4-5
	Практическое занятие 2	Модуль 1 0÷5 «Неудовлетворительно» - 0-1 «Удовлетворительно» - 2-3 «Хорошо» - 3-4 «Отлично» - 4-5
Владеть:		
- навыками анализа требований по защите средств вычислительной техники и автоматизированных систем на основе показателей защищенности; - навыками организации защиты информации ограниченного доступа в компьютерных сетях, соответствующей требованиям нормативных правовых актов и нормативных методических документов.	Лабораторная работа 1	Модуль 1 0÷5 «Неудовлетворительно» - 0-1 «Удовлетворительно» - 2-3 «Хорошо» - 3-4 «Отлично» - 4-5
	Лабораторная работа 2	Модуль 1 0÷5 «Неудовлетворительно» - 0-1 «Удовлетворительно» - 2-3 «Хорошо» - 3-4 «Отлично» - 4-5
	Лабораторная работа 3	Модуль 1 0÷5 «Неудовлетворительно» - 0-1 «Удовлетворительно» - 2-3 «Хорошо» - 3-4 «Отлично» - 4-5
	Лабораторная работа 4	Модуль 1 0÷5 «Неудовлетворительно» - 0-1 «Удовлетворительно» - 2-3 «Хорошо» - 3-4 «Отлично» - 4-5

	работа 4	0÷5 «Неудовлетворительно» - 0-1 «Удовлетворительно» - 2-3 «Хорошо» - 3-4 «Отлично» - 4-5
	Лабораторная работа 5	Модуль 1 0÷5 «Неудовлетворительно» - 0-1 «Удовлетворительно» - 2-3 «Хорошо» - 3-4 «Отлично» - 4-5
ОПК-9: Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности		
Знать:		
- принципы использования средств криптографической защиты информации при решении задач профессиональной деятельности; - методики использования технических средств защиты информации для решения практических задач обеспечения информационной безопасности.	Контрольная работа	Модуль 2 0÷25 «Неудовлетворительно» - 0-10 «Удовлетворительно» - 11-15 «Хорошо» - 16-20 «Отлично» - 21-25
Уметь:		
- использовать программно-аппаратные средства криптографической защиты информации для решения практических задач; - решать задачи защиты информации от утечки по техническим каналам, сетей и систем передачи информации.	Практическое занятие 3	Модуль 2 0÷5 «Неудовлетворительно» - 0-1 «Удовлетворительно» - 2-3 «Хорошо» - 3-4 «Отлично» - 4-5
	Практическое занятие 4	Модуль 2 0÷5 «Неудовлетворительно» - 0-1 «Удовлетворительно» - 2-3 «Хорошо» - 3-4 «Отлично» - 4-5
Владеть:		
- навыками установки и настройки программно-аппаратных средств криптографической защиты информации для решения практических задач; - навыками использования специальных технических средств при защите информации от утечки по техническим каналам, сетей и систем передачи информации.	Лабораторная работа 6	Модуль 2 0÷5 «Неудовлетворительно» - 0-1 «Удовлетворительно» - 2-3 «Хорошо» - 3-4 «Отлично» - 4-5
	Лабораторная работа 7	Модуль 2 0÷5 «Неудовлетворительно» - 0-1 «Удовлетворительно» - 2-3 «Хорошо» - 3-4 «Отлично» - 4-5
	Лабораторная работа 8	Модуль 2 0÷5 «Неудовлетворительно» - 0-1 «Удовлетворительно» - 2-3

		«Хорошо» - 3-4 «Отлично» - 4-5
	Экзамен	0-100 «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

Данная дисциплина формирует у обучающегося 2 компетенцию, которые связаны, взаимодействуют между собой и объективно оценить каждую в отдельности при ответе обучающегося на контрольный вопрос или при выполнении практического или лабораторного задания достаточно сложно.

Модуль 1 (50 баллов):

Модуль содержит 9 лекционных занятия, 2 практических и 5 лабораторных занятия. Знание лекционного материала оценивается по контрольной работе, состоящей из двух вопросов, максимальное количество баллов за контрольную работу составляет 15. За одно выполненное и защищенное практическое занятие обучающийся получает максимум по 5 баллов; за одну лабораторную работу - максимум 5 баллов. Общее максимальное количество баллов за модуль 1 составляет 50.

Вопросы для контрольной работы (ОПК-6):

1. Информация как главный ресурс научно-технического и социально-экономического развития общества.
2. Задачи обеспечения информационной безопасности телекоммуникационных систем.
3. Система передачи информации с шифрованием сообщений.
4. Три исторических этапа развития КСЗИ.
5. Симметричные и асимметричные КСЗИ.
6. Основные требования к КСЗИ.
7. Основные понятия криптографии: алфавит, открытый текст, закрытый текст (криптограмма), шифрование, расшифрование, секретный ключ.
8. Криптоанализ и дешифрование.
9. Теоретико-информационные основы криптозащиты сообщений.
10. Количественные меры информации.
11. Взаимная информация между криптограммой и ключом (первая криптотеорема Шеннона). Теоретическая стойкость КСЗИ.
12. Криптоанализ и дешифрование.
13. Правило Керкхоффа.
14. Криптография и теория чисел. Модулярная арифметика.
15. Операторы шифрования: общие свойства и требования.
16. Совершенная секретность и случайные ключи. Совершенный шифр Вернама. Информационная цена криптозащиты.
17. Избыточность сообщений и её роль в криптоанализе. Оценка расстояния единственности.
18. История появления шифров

19. Основные проблемы инженерно-технической защиты информации.
20. Представление сил и средств защиты информации в виде системы.
21. Основные параметры системы защиты информации
22. Цели и задачи защиты информации. Ресурсы, выделяемые на защиту информации.
23. Принципы защиты информации техническими средствами.
24. Организация формирования ключей в симметричных КСЗИ.
25. Особенности генерации ключей при блочном шифровании: случайные числа, равномерно распределенные случайные последовательности, псевдослучайные последовательности.
26. Линейные и нелинейные конгруэнтные генераторы.
27. Организация формирования ключей в асимметричных КСЗИ.
28. Стандарты на электронную (цифровую) подпись:
29. Цифровая подпись DSS,
30. Цифровая подпись ГОСТ Р34.10-94.
31. Цифровые подписи, основанные на симметричных криптосистемах.
32. Функции хеширования:ГОСТ Р34.11-94, MD5.
33. Функции хеширования: SHA.
34. Основные требования к электронной подписи.
35. Алгоритмы электронной подписи: электронная подпись на основе криптосистемы RSA,
36. Электронная подпись на основе шифра Эль-Гамала.
37. Анализ электронной цифровой подписи на основе криптосистемы Эль Гамала.
38. Криптоанализ шифра Виженера с известной длиной ключа
39. Методы средства ограничения доступа к компонентам ЭВМ
40. Надёжность средств защиты компонент;
41. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям
42. Методы средства хранения ключевой информации,
43. Типовые решения в организации ключевых систем;
44. Защита программ от излучения,
45. Способы встраивания средств защиты в программное обеспечение.

Практическое занятие №1 Криптоанализ и дешифрование..

Контрольные вопросы ПЗ№1 (ОПК-6):

1. Основные понятия криптографии: алфавит, открытый текст, закрытый текст (криптограмма), шифрование, расшифрование, секретный ключ.
2. Криптоанализ и дешифрование.
3. Теоретико- информационные основы криптозащиты сообщений.
4. Количественные меры информации.
5. Взаимная информация между криптограммой и ключом (первая криптотеорема Шеннона). Теоретическая стойкость КСЗИ.
6. Криптоанализ и дешифрование.
7. Правило Керкхоффа.
8. Криптография и теория чисел. Модулярная арифметика.

Практическое занятие №2 Операторы шифрования.

Контрольные вопросы ПЗ№2 (ОПК-6):

1. Операторы шифрования: общие свойства и требования.
2. Совершенная секретность и случайные ключи. Совершенный шифр Вернама. Информационная цена криптозащиты.
3. Избыточность сообщений и её роль в криптоанализе. Оценка расстояния единственности.
4. Представление сил и средств защиты информации в виде системы.

5. Основные параметры системы защиты информации

Лабораторная работа №1.

Контрольные вопросы ЛРН №1 (ОПК-6):

1. Моно и много алфавитные подстановки. Перестановки.
2. Простейшие алгоритмы шифрования и расшифрования.
3. Шифры Цезаря, Виженера.
4. Криптоанализ или атака на шифры Цезаря и Виженера.
5. Шифры на основе подстановки на алфавите и перестановки.
6. Принципы блочного многоаундового шифрования.

Лабораторная работа №2.

Контрольные вопросы ЛРН №2 (ОПК-6):

1. Понятие перестановки.
2. Понятие взаимно-однозначного отображения (гомо-морфизма).
3. Простая перестановка.
4. Усложненная перестановка. Гамильтоновы пути.
5. Шифр вертикальной перестановки.
6. Понятие перестановки. Двойная перестановка.
7. Шифрование с использованием алгебры матриц.

Лабораторная работа №3.

Контрольные вопросы ЛРН №3 (ОПК-6):

1. Организация секретной связи с закрытым каналом передачи секретного ключа.
2. Основные классы симметричных КСЗИ.
3. Схема Фейстеля.
4. Генерирование блочных шифров.
5. Блочный шифр DES, разновидности алгоритма DES.
6. Алгоритм RC6.

Лабораторная работа №4.

Контрольные вопросы ЛРН №4 (ОПК-6):

1. Цифровая подпись DSS.
2. цифровая подпись ГОСТ Р34.10-94.
3. Цифровые подписи, основанные на симметричных криптосистемах.
4. Механизм действия электронной цифровой подписи.
5. Функции хэширования.
6. Алгоритмы цифровой подписи.
7. Криптоанализ односторонних хэш-функций.

Лабораторная работа №5.

Контрольные вопросы ЛРН №5 (ОПК-6):

1. Системы шифрования с открытыми ключами.
2. Асимметричные системы.
3. Открытое распределение ключей.
4. Схема Диффи-Хеллмана. Криптосистема RSA.
5. Схема шифрования Эль-Гамала.
6. Криптография на эллиптических кривых. Криптоанализ шифра RSA.
7. Криптоанализ односторонних хэш-функций.

Модуль 2: (50 баллов):

Модуль содержит 4 лекционных занятия, 2 практических и 3 лабораторных занятий. Знание лекционного материала оценивается по контрольной работе, состоящей из двух вопросов, максимальное количество баллов за контрольную работу составляет 25. За выполненное и защищенное одно практическое занятие максимум 5 баллов. За выполненную и защищенную одну лабораторную работу обучающийся получает максимум 5 баллов. Общее максимальное количество баллов за модуль 2 составляет 50.

Вопросы для контрольной работы (ОПК-9):

1. Нормативно-правовые основы криптографической защиты информации.
2. Действующие стандарты криптографической защиты информации.
3. Федеральный закон об электронной подписи.
4. Нормативно-правовые акты ФСБ по обеспечению безопасности персональных данных с использованием СКЗИ.
5. Нормативно-правовые акты ФСБ по обеспечению функционирования и эксплуатации СКЗИ.
6. Виды работ и услуг, составляющих лицензируемую деятельность с использованием СКЗИ.
7. Порядок лицензирования деятельности с использованием СКЗИ.
8. Правила сертификации СКЗИ по требованиям ФСБ.
9. Классификация средств криптографической защиты информации.
10. Требования к средствам криптографической защиты информации.
11. Программные СКЗИ.
12. Аппаратные и программно-аппаратные СКЗИ.
13. Критерии выбора СКЗИ.
14. Основные принципы построения СКЗИ.
15. Принципы построения аппаратных СКЗИ.
16. Принципы построения программных и программно-аппаратных СКЗИ.
17. Основные подходы к обеспечению надежности СКЗИ
18. Средства криптографической защиты информации на персональном компьютере.
19. Задачи обеспечения информационной безопасности на персональном компьютере с использованием СКЗИ.
20. Криптографическая защита жестких дисков и съемных носителей.
21. Средства шифрования, встроенные в операционную систему Windows. Шифрование архиваторов.
22. СКЗИ свободного доступа.
23. СКЗИ от несанкционированного доступа.
24. Средства криптографической защиты сетевого взаимодействия.
25. Криптографические средства создания защищенных виртуальных сетей (VPN).
26. Технология построения криптозащищенных туннелей.
27. Криптографическая защита удаленного доступа к локальной сети.
28. СКЗИ для передачи данных в локальных сетях.
29. Сетевые протоколы криптографической защиты.
30. Персональные криптографические средства аутентификации.

Практическое занятие №3.

Контрольные вопросы ПЗ№3 (ОПК-9):

1. В чем суть объектной модели безопасности Windows? Что такое список контроля доступа и элемент списка контроля доступа. Приведите пример списка контроля доступа и элемента списка контроля доступа.
2. Что собой представляют разрешения NTFS? Как Вы понимаете наследование раз-

решений? Как можно отменить наследование разрешений? С помощью какого средства можно настроить разрешения NTFS?

3. Какие виды разрешений для папки существуют, какие действия позволяет выполнять каждое из этих разрешений?

4. Что происходит с разрешениями на файл при переносе файла и при копировании файла?

5. Опишите рациональную методику назначения прав на общие ресурсы пользователей и общие папки пользователей?

6. Если в каталоге обнаруживается файл, права на который не являются наследованными с родительского каталога, какие действия необходимо предпринять, чтобы исправить эту ситуацию?

7. Зачем нужны административные «шары» и каким образом их можно создать?

8. Если права на общий ресурс не эквивалентны правам NTFS – как формируются результирующие права доступа к ресурсу?

Практическое занятие №4.

Контрольные вопросы ПЗ№4 (ОПК-9):

1. Дайте определение дескриптора защиты, из каких элементов он состоит?

2. Что такой системный список контроля доступа? Какая информация в нем хранится?

3. Перечислите все этапы активации аудита доступа к файлу или папке NTFS.

4. Какие инструменты используются для настройки аудита и получения его результатов? Перечислите функции каждого из них.

5. Каким образом можно применить настройки групповой политики по активации аудита?

6. В каких случаях необходим аудит папок и файлов?

Лабораторная работа № 6.

Контрольные вопросы ЛР№6 (ОПК-9):

1. Для чего используется электронная подпись?

2. Что такое «сертификат ключа»? Для чего он предназначен?

3. Почему у сертификата есть срок действия?

4. В таких случаях сертификат необходимо отозвать досрочно, чтобы его невозможно было использовать случайно или со злоумышленными намерениями.

5. Как происходит наложение и проверка подписи? Изменяется ли при этом документ?

6. Возможно ли подделать открытый ключ?

7. Почему необходимы два ключа?

8. Кто занимается выдачей сертификатов электронной подписи (ЭП)? Каков механизм получения ЭП?

9. Что такое центр сертификации ключей?

10. В основе инфраструктуры открытых ключей (ИОК) лежит специальный субъект - центр сертификации ключей (ЦСК), основной целью которого является обеспечение безопасного обмена открытыми ключами между участниками электронного взаимодействия.

11. Права ЦСК?

12. Обязанности ЦСК?

13. Какие услуги предоставляет центр сертификации ключей на платной основе?

14. На каких условиях строятся отношения между центром сертификации и пользователями?

15. Можно ли передавать секретный ключ ЭП другим лицам на время отсутствия владельца ключа?

Лабораторная работа № 7.

Контрольные вопросы ЛР№7 (ОПК-9):

1. Какой ключ используется для подписи, какой – для шифрования?
2. Какие свойства документа обеспечивает наличие цифровой подписи?
3. Какие два способа добавления подписи к документу Word Вы знаете? Чем они отличаются?
4. Какие хранилища сертификатов имеются в операционной системе Windows? Для чего каждое из них предназначено?
5. Какие форматы экспорта сертификатов Вы знаете? Перечислите расширения файлов сертификатов.
6. Какой формат экспорта сертификатов позволяет экспортировать закрытый ключ? Какой формат экспорта Вы использовали в этой лабораторной работе и почему?

Лабораторная работа № 8

Контрольные вопросы ЛР№8 (ОПК-9):

1. Какой ключ используется для подписи, какой – для шифрования?
2. Какие свойства документа обеспечивает наличие цифровой подписи?
3. Какие два способа добавления подписи к документу Word Вы знаете? Чем они отличаются?
4. Какие хранилища сертификатов имеются в операционной системе Windows 7? Для чего каждое из них предназначено?
5. Какие форматы экспорта сертификатов Вы знаете? Перечислите расширения файлов сертификатов.
6. Какой формат экспорта сертификатов позволяет экспортировать закрытый ключ? Какой формат экспорта Вы использовали в этой лабораторной работе и почему?

Модуль «Курсовая работа» (100 баллов):

Тема курсовой работы:

«Криптоанализ шифра Виженера».

Для выполнения курсовой работы обучающиеся скачивают с методического раздела сайта СКФ МТУСИ Методические указания по выполнению курсовой работы по дисциплине «Методы и средства криптографической защиты информации»/ П.С. Шухардин А.Н., Юхнов В.И. – Ростов-на -Дону: Изд-во СКФ МТУСИ, 2025. – 53 с

Модуль посвящен выполнению задания на курсовую работу. Максимальное количество баллов за выполненную и защищенную курсовую работу составляет 100.

Курсовая работа выполняется в процессе освоения компетенций ОПК-6, ОПК-9 и ее итоговая оценка характеризует заключительный этап их освоения. Ввиду сложности определения вклада той или иной компетенции в курсовую работу, для упрощения процедуры оценивания будем считать, что их вклад в курсовую работу одинаков, а максимальное количество баллов за каждую компетенцию может составить 50.

Критерии оценки курсового проекта приведены в таблице 1.

Таблица 1 – Критерии оценки курсового проекта

№п/п	Оцениваемые параметры	Оценка в баллах
1.	Выполнение задания на курсовое проектирование: - Задание выполнено в полном объеме, каждый рассматриваемый вопрос раскрыт полностью, спроектированная система спутникового приема соответствуют предъявляемым к ней требованиям.	20

№п/п	Оцениваемые параметры	Оценка в баллах
	- Задание выполнено в полном объеме, один или несколько рассматриваемых вопросов раскрыты неполно, спроектированная система спутникового приема соответствуют предъявляемым к ней требованиям.	10
	- Один или несколько пунктов задания не выполнены или выполнены не в полном объеме	0
2.	Использование демонстрационного материала: - демонстрационный материал включает в себя технические требования к системе спутникового приема, структурную схему системы, зону покрытия спутника, перечень принимаемых спутников, перечень принимаемых русскоязычных программ, внешний вид и технические характеристики оборудования. - демонстрационный материал включает в себя технические требования к системе спутникового приема, структурную схему системы, зону покрытия спутника, внешний вид и технические характеристики оборудования - демонстрационный материал включает в себя технические требования к системе спутникового приема, зону покрытия спутника, перечень принимаемых спутников, технические характеристики оборудования; - демонстрационный материал не отражает основных этапов проектирования.	20 14 8 2
3.	Оформление результатов работы - курсовой проект оформлен в полном соответствии с ЕСКД; - курсовой проект оформлен с незначительными отклонениями от ЕСКД; - оформление проекта не соответствует требованиям ЕСКД.	20 10 4
4.	Качество ответов на вопросы: - отвечает на вопросы; - не может ответить на большинство вопросов; - не может четко ответить на вопросы.	40 24 13

Обучающийся, набравший минимум баллов по одному из пунктов 1 – 3, получает по курсовому проекту оценку «неудовлетворительно». Обучающийся, набравший от 41 до 60 баллов, получает оценку «удовлетворительно», от 61 до 80 баллов, получает оценку «хорошо», от 81 балла и выше – оценку «отлично».

1.3.2 Вопросы, выносимые на экзамен по дисциплине «Методы и средства криптографической защиты информации» (промежуточная аттестация)

1. Понятия "информационная безопасность" и "защита информации". Основные составляющие информационной безопасности.(ОПК-6)
2. Объекты защиты. Категории и носители информации (ОПК-6)
3. Средства защиты информации (ОПК-6)
4. Криптография. Основные термины и определения (ОПК-6)
5. Классификация криптографических систем (ОПК-6)
6. Шифры замены. Основные методы шифрования. (ОПК-6)
7. Шифры перестановки. Основные методы шифрования. (ОПК-6)
8. Шифры гаммирования. Основные методы шифрования. (ОПК-6)
9. Шифры гаммирования. Способы генерации гаммы. Генераторы гамм. (ОПК-6)
10. Схема режима шифрования DES-ECB.(ОПК-6)
11. Схема режима шифрования DES-CBC. (ОПК-6)
12. Схема режима шифрования DES-CPB и DES-OFB.(ОПК-6)
13. Тройной DES. Сферы применения различных режимов DES. (ОПК-6)
14. Схема режима шифрования простой замены ГОСТ 28147-89.(ОПК-6)

15. Шифрование с открытым ключом. Основные понятия.(ОПК-6)
16. Алгоритм шифрования RSA.(ОПК-6)
17. Алгоритм шифрования Эль-Гамала.(ОПК-6)
18. Алгоритм шифрования на основе задачи об укладке ранца. (ОПК-6)
19. Эллиптические кривые. Основные понятия. Сложение и умножение точки (ОПК-6)
20. Алгоритм шифрования на основе эллиптических кривых. (ОПК-6)
21. Хэш-функции. Основные понятия и разновидности. (ОПК-6)
22. Хэш-функция. MD5. (ОПК-6)
23. Криптографические протоколы. Основные понятия. (ОПК-6)
24. Протоколы обмена ключами. (ОПК-6)
25. Протоколы аутентификации. Разновидности и краткая характеристика. (ОПК-6)
26. Парольная идентификация/аутентификация. (ОПК-6)
27. Протокол идентификации/аутентификации на основе шифрования с открытым ключом. (ОПК-6)
28. Сервер аутентификации Kerberos. (ОПК-6)
29. Идентификация/аутентификация с помощью биометрических данных. (ОПК-6)
30. Идентификационные карты (ID-cards) и электронные ключи. (ОПК-6)
31. Электронная цифровая подпись. Общие сведения и разновидности ЭЦП. (ОПК-6)
32. ЭЦП на базе алгоритма RSA. (ОПК-6)
33. Алгоритм цифровой подписи ГОСТ 34.10-94. (ОПК-6)
34. Алгоритм цифровой подписи ГОСТ 34.10-2001. (ОПК-6)
35. Нормативно-правовые основы криптографической защиты информации (ОПК-9).
36. Действующие стандарты криптографической защиты информации (ОПК-9).
37. Федеральный закон об электронной подписи (ОПК-9).
38. Виды работ и услуг, составляющих лицензируемую деятельность с использованием СКЗИ (ОПК-9).
39. Порядок лицензирования деятельности с использованием СКЗИ (ОПК-9).
40. Классификация средств криптографической защиты информации (ОПК-9).
41. Требования к средствам криптографической защиты информации (ОПК-9).
42. Программные СКЗИ (ОПК-9).
43. Аппаратные и программно-аппаратные СКЗИ (ОПК-9).
44. Основные принципы построения СКЗИ (ОПК-9).
45. Принципы построения аппаратных СКЗИ (ОПК-9).
46. Основные подходы к обеспечению надежности СКЗИ (ОПК-9).
47. Средства криптографической защиты информации на персональном компьютере (ОПК-9).
48. Криптографическая защита жестких дисков и съемных носителей (ОПК-9).
49. Средства шифрования, встроенные в операционную систему Windows. Шифрование архиваторов (ОПК-9).
50. Криптографические средства создания защищенных виртуальных сетей (VPN) (ОПК-9).

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

Порядок и методика проведения текущего контроля и промежуточной аттестации.

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 лабораторным работам и практическим занятиям для оценки практических навыков;
- промежуточная аттестация по дисциплине – в форме защиты курсовой работы и экзамена.

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

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

- 2-й этап выполняется по окончании каждой лабораторной работы (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 баллы в рамках текущего контроля 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 2.

Таблица 2 - Распределение баллов по блокам модулей дисциплины «Методы и средства криптографической защиты информации»

Модуль	Всего баллов (Максимальное значение)	Теоретический блок (Контрольная работа)	Практический блок (Распределение баллов по занятиям)
Модуль 1	50	15	35=5+5+5+5+5+5+5
Модуль 2	50	25	25=5+5+5+5+5
Модуль – КР	100	40	60 = 20+20+20
Экзамен	100	100	

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 защиты курсовой работы и экзамена.

Защита курсовой работы проводится по расписанию промежуточной аттестации. Результаты аттестации заносятся в ведомость и зачетную книжку обучающегося.

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 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 Курс: 3 Дисциплина: Методы и средства криптографической защиты информации		
Билет №1 1. Понятия "информационная безопасность" и "защита информации". Основные составляющие информационной безопасности. 2. Основные понятия криптологии. Криптография и криптоанализ. Стеганография. к.т.н., доцент _____ Шухардин А.Н. .«___» _____ 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, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Тестовые задания позволяют оценить уровень сформированности 2-х компетенций ОПК-6 и ОПК-9.

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 по каждой компетенции равно 20. Всего 40 заданий.

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

ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

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

№ задания	Тексты заданий
1	Какова главная цель политики информационной безопасности организации? (один вариант) 1. Увеличить скорость сети. 2. Установить правила защиты и распределение ответственности. 3. Заменить все ПО на отечественное. 4. Запретить удалённую работу.
2	Какие документы относятся к нормативно-правовой базе защиты информации в РФ? (выберите все подходящие) 1. Федеральный закон об электронной подписи. 2. Ведомственные акты ФСТЭК/ФСБ. 3. RFC по протоколам Интернета. 4. Трудовой кодекс РФ в части дисциплинарной ответственности.
3	Что обычно включает «модель нарушителя»? (выберите все подходящие) 1. Ресурсы и мотивация нарушителя. 2. Список поставщиков оборудования. 3. Предполагаемые векторы атак. 4. Допустимый простой сервиса.
4	Какой контроль относится к организационным? (один вариант) 1. Экран блокировки ОС. 2. Видео-наблюдение в серверной. 3. Регламент управления доступом и роли. 4. Модуль TPM.
5	Что является типичным результатом анализа рисков? (один вариант) 1. План обработки рисков. 2. Схема адресного пространства сети.

№ задания	Тексты заданий
	3. Список MAC-адресов сотрудников. 4. Детальный отчет по нагрузочному тесту.
6	Какие меры относятся к управлению доступом? (выберите все подходящие) 1. RBAC (ролевая модель). 2. Разделение полномочий (SoD). 3. Сжатие логов. 4. Политика минимально необходимых прав.
7	Что относится к обязательным требованиям при обращении с инцидентами ИБ? (выберите все подходящие) 1. Регистрация и классификация инцидентов. 2. Назначение ответственных и эскалация. 3. Удаление всех логов для конфиденциальности. 4. Пост-анализ и корректирующие действия.
8	Что относится к защитным мерам персональных данных? (выберите все подходящие) 1. Локализация БД ПДн в любой стране. 2. Разграничение доступа по ролям. 3. Критерии уровня защищенности в зависимости от угроз. 4. Использование «общих» учетных записей для упрощения.
9	Какой документ определяет правила обращения с носителями информации? (один вариант) 1. Политика управления носителями. 2. Реестр активов. 3. Паспорт СКЗИ. 4. Регламент резервного копирования.
10	Что относится к требованиям к журналированию? (выберите все подходящие) 1. Сохранность и целостность журналов. 2. Хранение журналов бессрочно. 3. Своевременность и синхронизация времени. 4. Доступность журналов только уполномоченным.

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

№ задания	Тексты заданий
11	Соотнесите пример и тип контроля 1. Регламент по управлению доступом. 2. СКУД и охранная сигнализация. 3. Межсетевой экран уровня L3/L4. 4. Средства DLP-класса в ОС. Варианты для сопоставления: А. Организационный Б. Технический. В. Физический. Г. Программный.
12	Соотнесите характеристику и модель управления доступом 1. Политики на основе атрибутов 2. Дискреционная (владелец определяет доступ) 3. Мандатная (метки конфиденциальности) 4. Ролевая (права через роли) Варианты для сопоставления: А. DAC Б. MAC В. RBAC Г. ABAC
13	Соотнесите действие и этап управления инцидентами: 1. Устранение последствий и возврат к штатному режиму 2. Разбор причин и корректирующие меры 3. Фиксация события и уведомление ответственных 4. Определение приоритета и маршрутизация

№ задания	Тексты заданий
	применение: А. Обнаружение и регистрация Б. Классификация и эскалация В. Ликвидация и восстановление Г. Последующий анализ
14	Соотнесите содержание и документ: 1. Критичные процессы и сценарии восстановления 2. Список информационных ресурсов и владельцев 3. Высокоуровневые цели и принципы защиты 4. Соответствие ролей и прав доступа характерное свойство А. Политика ИБ Б. Реестр активов В. Матрица распределения ролей. Г. План непрерывности бизнеса (BCP)

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

Инструкция: Прочитайте текст и установите правильную последовательность

№ задания	Тексты заданий
15	Определите порядок внедрения системы управления доступом: 1. Инвентаризация активов и прав 2. Определение ролей и принципов минимальных прав 3. Настройка механизмов контроля и выдача прав 4. Аудит и корректировка
16	Последовательность разработки политики ИБ: 1. Анализ нормативных требований и рисков 2. Формулирование целей и принципов 3. Согласование и утверждение 4. Коммуникация и обучение персонала
17	Ввод в эксплуатацию СЗИ по регламенту: 1. Установка и настройка 2. Проведение приемочных испытаний 3. Оформление эксплуатационной документации 4. Передача в промышленную эксплуатацию

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

Инструкция: Прочитайте текст и запишите обоснованный ответ

№ задания	Тексты заданий
18	Вставьте термин: Документ, описывающий гипотетические возможности оппонента, его мотивацию, ресурсы и предполагаемые векторы атак — это _____.
19	Вставьте термин: Совокупность правил и требований к защите информации в организации, определяющая ответственность и принципы — это _____.
20	Вставьте термин: Процесс систематической оценки вероятности и последствий угроз для активов — это _____.

Система оценивания выполнения тестовых заданий по компетенции ОПК-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

ОПК-9

Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности

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

№ задания	Тексты заданий
1	Какой режим блочного шифра обеспечивает одновременно шифрование и аутентификацию (AEAD)? (один вариант) 1. ECB 2. CBC 3. CTR 4. GCM
2	Какие средства относятся к программно-аппаратным для КЗИ на рабочей станции? (выберите все подходящие) 1. TPM/чип доверенной платформы 2. HSM/аппаратные модули защиты ключей 3. ZIP-архиватор 4. Смарт-карта/токен
3	Что характерно для PKI? (выберите все подходящие) 1. Центр сертификации (CA) 2. Сертификаты X.509 3. DHCP-сервер 4. Список отозванных сертификатов (CRL)/OCSP
4	Какой алгоритм обычно применяют для выработки кода аутентичности сообщения? (один вариант) 1. HMAC 2. PBKDF2 3. RSA 4. Diffie–Hellman
5	Что верно о настройке VPN с IPsec? (выберите все подходящие) 1. Используются протоколы IKE для согласования параметров 2. ESP обеспечивает шифрование/аутентификацию трафика 3. TLS всегда обязателен для IPsec 4. Применяются политики/списки трафика (selectors)
6	Какой параметр критичен для безопасного использования потоковой гаммы? (один вариант) 1. Повторное использование nonce/IV недопустимо 2. Размер окна TCP 3. MTU канала 4. Тип файловой системы
7	Что верно для шифрования диска BitLocker/аналогов? (выберите все подходящие) 1. Защита «на покое» (at rest) 2. Возможность интеграции с TPM и PIN 3. Требуется обязательного подключения к Интернету 4. Поддерживает шифрование съёмных носителей
8	Что является хорошей практикой при управлении ключами? (выберите все подходящие) 1. Ротация ключей 2. Разделение ключей по назначению (шифрование/подпись) 3. Хранение приватных ключей в общем сетевом каталоге 4. Резервное копирование и политика отзыва
9	Для электронной подписи на эллиптических кривых (ECDSA) верно: (выберите все подходящие) 1. Требуется надёжного генератора случайных k 2. Основана на трудности дискретного логарифмирования на ЭК 3. Использует факторизацию больших целых 4. Компактные ключи при сопоставимой безопасности
10	Что относится к защите от утечек по техническим каналам? (выберите все подходящие)

№ задания	Тексты заданий
	1. Экранирование и заземление 2. Режимы «безопасной печати» 3. Установка обновлений ОС 4. Фильтрация побочных электромагнитных излучений

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

№ задания	Тексты заданий
11	Соотнесите средство и задачу: 1. HSM 2. Diffie–Hellman 3. HMAC 4. TLS/IPsec Варианты для сопоставления: А. Хранение ключей высокой критичности Б. Согласование общего секрета по незащищенному каналу В. Аутентификация сообщения Г. Шифрование при передаче
12	Соотнесите особенность и режим/алгоритм: 1. Поточковый счетчик, параллелится 2. AEAD-режим на блочном шифре 3. Современный AEAD на потоке+MAC 4. Требуется случайного IV и корректного паддинга Варианты для сопоставления: А. CBC Б. CTR В. GCM Г. ChaCha20-Poly1305
13	Соотнесите роль и компонент PKI: 1. Проверка статуса отзыва сертификата 2. Регистрация и верификация заявителей 3. Выпуск и подписание сертификатов 4. Безопасное расположение закрытых ключей Варианты для сопоставления: А. CA Б. RA В. CRL/OCSP Г. Хранилище ключей
14	Соотнесите область применения и протокол/технология: 1. Защита Wi-Fi в корпоративной сети 2. Туннелирование уровня приложений/управления серверами 3. Сетевой туннель L3/L4 с шифрованием 4. VPN на базе TLS-сертификатов Варианты для сопоставления: А. WPA2-Enterprise Б. OpenVPN (TLS) В. IPsec (ESP) Г. SSH

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

Инструкция: Прочитайте текст и установите правильную последовательность

№ задания	Тексты заданий
15	Настройка TLS на веб-сервере (упрощённо): 1. Генерация пары ключей и CSR 2. Получение сертификата от СА 3. Настройка шифросюит в конфигурации 4. Включение HSTS/перенаправление на HTTPS и перезапуск
16	Развертывание VPN на IPsec-шлюзах (site-to-site): 1. Обмен сертификатами/настройка IKE профилей 2. Определение трафика для туннелирования (selectors/policies) 3. Настройка ESP/шифросюит и аутентификации 4. Тестирование, мониторинг и резервирование
17	Процесс подписания и проверки электронного документа: 1. Вычислить хэш сообщения 2. Выработать подпись закрытым ключом отправителя 3. Передать сообщение и подпись 4. Проверить подпись открытым ключом, сравнить хэш

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

Инструкция: Прочитайте текст и запишите обоснованный ответ

№ задания	Тексты заданий
18	Класс методов, при которых из пароля выводится ключ с помощью итеративной функции растяжки — это _____.
19	Выберите термин, которому соответствует определение: Защищённый аппаратный модуль для генерации, хранения и операций с ключами — это _____.
20	Вставьте термин: Неповторяющееся значение, используемое для предотвращения повторного использования потоковой гаммы — это _____.

Система оценивания выполнения тестовых заданий по компетенции ОПК-9

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 контроля и промежуточной аттестации 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 лабораторным работам

Лабораторные занятия по любой учебной дисциплине проводятся в соответствии с рабочей программой этой учебной дисциплины в установленные расписанием часы.

Инструктаж по технике безопасности, правилам пожарной безопасности и правилам внутреннего распорядка в лаборатории проводится преподавателем на первом лабораторном занятии. На этом же занятии обучающимся сообщаются:

- программа всего предстоящего лабораторного цикла;
- условия взаимодействия обучающихся с преподавателем в процессе выполнения лабораторных работ;
- условия контроля самостоятельной работы обучающихся, включая правила оформления отчетов по лабораторным работам и их последующей защиты;
- другая необходимая информация.

Организация лабораторных работ включает:

- самостоятельную внеаудиторную подготовку обучающегося к выполнению каждой отдельной лабораторной работы в соответствии с ее программой в рамках часов, выделенных на самостоятельную проработку материала в программе дисциплины;
- входной контроль преподавателем степени подготовленности каждого обучающегося к выполнению лабораторных работ;
- выполнение программы лабораторных работ в полном объеме;
- оформление отчета и его защиту каждым обучающимся в установленные сроки;
- формирование преподавателем рейтингов каждого из обучающихся по результатам выполнения и защиты им отдельных лабораторных работ и их циклов (используется Модульно-рейтинговая система).

Оценка качества выполнения лабораторных работ каждым обучающимся производится преподавателем отдельно за подготовку к работе, ее выполнение и защиту.

2.3 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.

2.3. Методические указания для обучающихся по подготовке курсовой работы

Курсовая работа включает в себя:

- титульный лист;
- содержание;
- перечень условных обозначений (при необходимости);
- основную текстовую часть работы (введение, основную часть, заключение);
- список использованных источников;
- приложения (при необходимости).

По объему страниц «Введение» может достигать 3 страниц. Во введении отражаются следующие основные моменты:

- актуальность выбранной темы,
- теоретическое и практическое значение выбранной темы, ее актуальность;
- степень разработанности проблемы (краткий обзор и анализ экономической литературы по выбранной теме курсовой работы);
- обосновывается и определяются цель, а также конкретные задачи исследования;
- обоснование логической последовательности раскрываемых вопросов, общего порядка исследования и структуры работы.

Порядок выполнения курсовой работы приведен в методических материалах по ее выполнению.

Критерии оценки курсовой работы приведены в оценочных материалах дисциплины.

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;
- подготовку к лабораторным работам (практическим занятиям);
- изучение учебной и научной литературы;
- решение задач, выданных на практических занятиях;
- подготовку 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 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.

Постановку задачи обучаемым на проведение самостоятельной работы преподаватель осуществляет на одном из занятий, предшествующем данному.

Методику самостоятельной работы все обучаемые выбирают индивидуально.

Обучающимся очной формы обучения при освоении вопросов для самостоятельного изучения, представленных в подразделе 4.1 настоящей рабочей программы, рекомендуется соблюдать последовательность их изучения, представленную в таблице.

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

№	Темы, разделы, вынесенные на самостоятельную подготовку, вопросы для подготовки к практическим и лабораторным занятиям; курсовые работы, содержание контрольных работ; рекомендации по использованию литературы, ЭВМ и др.	Часов всего: 28	Неделя
Модуль 1			
1	История появления шифров	2	1-2
2	Основные этапы жизненного цикла вирусов; объекты внедрения, режимы функционирования и специальные функции вирусов	2	3-4
3	Схемы заражения файлов; схемы заражения загрузчиков; способы маркировки, используемые вирусами	4	5-7
Модуль 2			
4	Анализ структуры и принципов функционирования вычислительных сетей с позиции обеспечения информационной безопасности	4	7-8
5	Угрозы информационно-программному обеспечению, характерные только для распределённой вычислительной среды	4	8-10
6	Использование криптографических методов для защиты данных, циркулирующих в вычислительной сети	4	10-13
7	Методы средства ограничения доступа к компонентам ЭВМ	4	14
8	Надёжность средств защиты компонент; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям	2	15
9	Методы средства хранения ключевой информации, типовые решения в организации ключевых систем; защита программ от излучения, способы встраивания средств защиты в программное обеспечение.	2	16-17

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