

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» 04 2026 г.

Рабочая программа дисциплины

Б1.О.36.02 Криптографические протоколы

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/семестр
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	4	144/8
Контактная работа, в том числе (по семестрам, курсам):		72/8
Лекции		36/8
Лабораторных работ		
Практических занятий		36/8
Семинаров		
Самостоятельная работа		72/8
Контроль		
Число контрольных работ (по курсам)		
Число КР (по семестрам, курсам)		
Число КП (по семестрам, курсам)		
Число зачетов с оценкой с разбивкой по семестрам (курсам)		1/8
Число экзаменов с разбивкой по семестрам (курсам)		

Программу составил:

Кандидат технических наук, доцент, доцент Шухардин А.Н.

Рабочая программа дисциплины

«Криптографические протоколы»

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 учебного плана

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

Рассмотрена и одобрена на заседании кафедры

Информационной безопасности

Протокол от «28» 04 2026 г. № 9

И.О. Зав. кафедрой _____ Жуковский А.Г.

1. Цели изучения дисциплины

Целью освоения дисциплины является формирование у обучаемых знаний в области существующих подходов к анализу и синтезу криптографических протоколов, с государственными и международными стандартами в этой области.

Задачи освоения дисциплины:

- формирование знаний, умений и навыков, позволяющих анализировать, создавать и использовать криптографические протоколы для защиты информации,
- освоение принципов корректного применения современных защищенных информационных технологий.

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-8: Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности
Знать:
- нормативные и методические материалы по вопросам оценки уровня защищенности объекта защиты информации; - перечень необходимых вопросов по выбору справочной литературы по вопросам обеспечения информационной безопасности.
Уметь:
- осуществлять подбор нормативных и методических материалов по вопросам применения средств защиты информации; - осуществлять изучение и обобщение научно-технической литературы, составлять обзор по вопросам обеспечения информационной безопасности.
Владеть:
- навыками работы с нормативными и методическими материалами по вопросам применения средств защиты информации; - навыками работы со справочной и научно-технической литературой по вопросам обеспечения информационной безопасности.
ОПК-9: Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности
Знать:
- национальные стандарты Российской Федерации в области криптографической защиты информации и сферы их применения; - основные математические методы и алгоритмы шифрования, расшифрования и дешифрования сообщений; - виды криптографических протоколов и их место в комплексной системе защиты информации; - основные виды средств криптографической защиты информации (СКЗИ), включая блочные и поточные системы шифрования, криптографические системы с открытым ключом, криптографические хеш- функции и криптографические протоколы; - принципы функционирования программных средств криптографической защиты информации; - алгоритмы электронной (цифровой) подписи в телекоммуникационных системах.
Уметь:
- анализировать угрозы безопасности информации в компьютерных сетях; - использовать криптографические протоколы, применяемые в компьютерных сетях.
Владеть:
- навыками анализа и оценки угроз информационной безопасности объекта информатизации; - навыками установки программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты 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.29 «Методы и средства криптографической защиты информации»
2	Б1.О.14 «Информационные технологии и программирование»
3	Б1.О.06 «Высшая математика»
4	Б1.О.13 «Теория вероятности и математическая статистика»
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Б1.О.36.06 «Администрирование средств защиты информации в компьютерных системах и сетях»
2	Б1.О.30 «Моделирование систем защиты информации»

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 144 часов, 72 аудиторных часов, 72 часов самостоятельной работы)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
Курс 4, Семестр 8					
Модуль 1. Криптографические протоколы и их классификация (36+36) часов					
1.1	Лекция №1. КРИПТОГРАФИЧЕСКОГО ПРОТОКОЛЫ. Роль криптографических протоколов в системах защиты информации. Свойства протоколов, характеризующие их безопасность. Основные виды уязвимостей. Подходы к классификации криптографических протоколов. Подходы к моделированию криптографических протоколов	Лек1	2	ОПК-8 ОПК-9	Л1.1 Л1.2
1.2	Лекция №2. Понятие уязвимости и атаки на криптографический протокол. Основные виды криптографических систем.	Лек2	2	ОПК-8 ОПК-9	Л1.1 Л1.2
1.3	Практическое занятие № 1 Использование симметричных и асимметричных шифрсистем для построения криптографических протоколов. Примеры. Основные подходы к автоматизации анализа протоколов.	ПЗ1	4	ОПК-8 ОПК-9	Л3.1
1.4	Лекция №3. КРИПТОГРАФИЧЕСКИЕ ХЕШ-ФУНКЦИИ. Хэш-функции MD-5, семейство SHA	Лек3	2	ОПК-8 ОПК-9	Л1.1 Л1.2
1.5	Практическое занятие № 2 Функции хеширования: ГОСТ Р34.11-94, MD5, SHA	ПЗ2	4	ОПК-8 ОПК-9	Л3.1
1.6	Лекция № 4 СХЕМЫ ЦИФРОВОЙ ПОДПИСИ. Схемы цифровой подписи на основе симметричных и асимметричных шифрсистем. Схемы Эль-Гамала, Нюберг-Рюппеля и Шнорра, их свойства Семейство схем типа ЭльГамала.	Лек4	2	ОПК-9	Л1.1 Л1.2
1.7	Лекция № 5	Лек5	2	ОПК-9	Л1.1

	Одноразовые подписи. Схемы конфиденциальной цифровой подписи и подписи вслепую. Подписи с обнаружением подделки.				Л1.2
1.8	Практическое занятие №3 Стандарты США и России электронной цифровой подписи.	ПЗ3	4	ОПК-8 ОПК-9	ЛЗ.1
198	Лекция №6 ПРОТОКОЛЫ ГЕНЕРАЦИИ И ПЕРЕДАЧИ КЛЮЧЕЙ Протоколы на основе симметричных и асимметричных шифрсистем. Двух и трех сторонние протоколы передачи и распределения ключей. Функции доверенной третьей стороны и выполняемые ею роли.	Лек6	2	ОПК-9	Л1.1 Л1.2
1.9	Лекция № 7. СХЕМЫ ПРЕДВАРИТЕЛЬНОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ. Протокол открытого распределения ключей Диффи-Хеллмана и способы его защиты от атаки «противник в середине». Аутентифицированные протоколы открытого распределения ключей.	Лек7	2	ОПК-9	Л1.1 Л1.2
1.8	Практическое занятие № 4 Протокол открытого распределения ключей Диффи-Хеллмана.	ПЗ4	4	ОПК-9	ЛЗ.1
1.9	Лекция № 8. Групповые протоколы. Протоколы разделения секрета и распределения ключей для телеконференции.	Лек8	2	ОПК-9	Л1.1 Л1.2
1.10	Практическое занятие № 5 Групповые протоколы. Протоколы разделения секрета и распределения ключей для телеконференции	ПЗ5	4	ОПК-9	ЛЗ.1
1.11	Федеральный закон Российской Федерации «Об электронной подписи» 6.04.2011г. № 63-ФЗ РФ Нормативно-правовые акты Российской Федерации о ведении электронного документооборота.	СРС	36	ОПК-8 ОПК-9	Л1.1 Л1.2
Модуль 2 Прикладные криптографические протоколы (36+36)					
2.1	Лекция №9. Протоколы идентификации. Протоколы идентификации на основе паролей, протоколы “рукопожатия” и типа «запрос-ответ»..	Лек9	2	ОПК-8 ОПК-9	Л1.1 Л1.2
2.2	Лекция № 10. Идентификация с использованием систем открытого шифрования. Понятие протоколов интерактивного доказательства и доказательства знания. Протоколы Фиата-Шамира, Шаума, Шнорра и Окамото.	Лек10	2	ОПК -9	Л1.1 Л1.2
2.3	Лекция № 11. Связь между протоколами цифровой подписи и протоколами идентификации. Протоколы с самосертифицируемыми открытыми ключами, построенными на основе идентификаторов.	Лек11	2	ОПК-8 ОПК-9	Л1.1 Л1.2
2.4	Практическое занятие № 6 Протоколы идентификации.	ПЗ6	4	ОПК-9	ЛЗ.1

2.5	Лекция № 12. Протоколы с нулевым разглашением Протоколы решения математических задач. Протокол привязки к биту. Игровые протоколы. Подбрасывание монеты по телефону. Протоколы подписания контрактов.	Лек12	2	ОПК-8 ОПК-9	Л1.1 Л1.2
2.6	Лекция № 13. Сертифицированная электронная почта. Аргумент с нулевым разглашением. Схемы электронного голосования.	Лек13	2	ОПК-8 ОПК-9	Л1.1 Л1.2
2.7	Практическое занятие №7 Протоколы решения математических задач.	ПЗ7	4	ОПК-9	Л3.1
2.8	Лекция № 14. Базовый протокол с нулевым разглашением (Жан-Жак Кискате (Jean-Jfcques Quisquater) и Луи Гилу (Louis Guillou)).	Лек14	2	ОПК-8 ОПК-9	
2.9	Практическое занятие № 8 Схемы электронного голосования	ПЗ8	2	ОПК-8 ОПК-9	Л3.1
2.10	Лекция № 15. Особенности построения семейства протоколов IPsec	Лек15	2	ОПК-8 ОПК-9	Л1.1 Л1.2
2.11	Лекция № 16. Протоколы SSL/TLS и особенности их реализации.	Лек16	2	ОПК-8 ОПК-9	Л1.1 Л1.2
2.12	Практическое занятие № 9 Особенности построения семейства протоколов IPsec. Протоколы SSL/TLS и особенности их реализации.	ПЗ9	4	ОПК-8 ОПК-9	Л3.1
2.13	Лекция № 17. Электронные платежи и электронные монеты. Криптовалюты и блокчейн	Лек 17	4	ОПК-8 ОПК-9	Л1.1 Л1.2
2.14	Практическое занятие № 10 Криптовалюты.	ПЗ10	2	ОПК-8 ОПК-9	Л3.1
2.16	Анализ моделей нарушителя; угрозы информационно-программному обеспечению вычислительных систем и их классификация. Использование криптографических методов для защиты данных, циркулирующих в вычислительной сети.	СРС	36	ОПК-8 ОПК-9	Л1.1 Л1.2
	Зачет с оценкой			ОПК-8 ОПК-9	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Л3.2
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	Лапонина О.Р., В.А. Сухомлина	Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия : учебное пособие	М.: ИНТУИТ, Ай Пи Ар Медиа, 2024— 605 с.	Э1
Л1.2	Бабаш А.В.	Криптографические методы защиты	М.: РИОР:	Э2

		информации. Том 1: учебно-методическое пособие	ИНФРА-М, 2021. — 413 с.	
5.1.2. Дополнительная литература				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л2.1	Косолапов Ю.В.	Криптографические протоколы на основе линейных кодов: учебное пособие	Ростов-на-Дону, Таганрог: Изд-во ЮФУ, 2020. — 98 с.	Э3
Л2.2	Маршаков Д.В., Д.В. Фахти	Методы и средства криптографической защиты информации. Практический курс: учебное пособие	М.: ИНФРА-М, 2022. — 76 с	Э4
5.1.3. Учебно-методическое обеспечение				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л3.1	Енгибарян И.А.	Методические указания по проведению практических занятий по дисциплине «Криптографические протоколы»	РнД: СКФ МТУСИ, 2019	Э5
5.2. Электронные образовательные ресурсы				
Э1	: https://www.iprbookshop.ru/142292.html			
Э2	https://znanium.com/catalog/product/1215714			
Э3	https://www.iprbookshop.ru/100176.html			
Э4	https://znanium.ru/catalog/product/1891129			
Э5	https://elib.mtuci.ru/view.php?book_id=170074			
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	Национальный открытый университет «ИНТУИТ» - https://intuit.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	ОС Linux, ОС Window			
П.2	Word processor Microsoft Word or LibreOffice Writer или аналог.			
П.3	Kaspersky Endpoint Security.			

6. Материально-техническое обеспечение дисциплины

6.1 МТО лекционных занятий	
1	Лекционная аудитория, оборудованная интерактивной доской, проектором
6.2 МТО 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
6.3 МТО рубежных контролей, экзамена	
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, прочесть задание, оформить ответ, общаться с преподавателем).

10. Дополнения и изменения в Рабочей программе

Лист актуализации рабочей программы дисциплины «Криптографические протоколы Б1.О.36.02» 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-8: Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности		
Знать:		
- нормативные и методические материалы по вопросам оценки уровня защищенности объекта защиты информации.	Теоретический блок (контрольная работа 1)	Модуль 1 0÷25 «Неудовлетворительно» - 0-10 «Удовлетворительно» - 11-15 «Хорошо» - 16-20 «Отлично» - 21-25
- перечень необходимых вопросов по выбору справочной литературы по вопросам обеспечения информационной безопасности;	Теоретический блок (контрольная работа 2)	Модуль 2 0÷25 «Неудовлетворительно» - 0-10 «Удовлетворительно» - 11-15 «Хорошо» - 16-20 «Отлично» - 21-25
Уметь:		
- осуществлять подбор нормативных и методических материалов по вопросам применения средств защиты информации;	Практическое занятие 1 – 5 (за занятие максимально 5 баллов)	Модуль 1 0÷5 за каждое ПЗ «Неудовлетворительно» - 0-1 «Удовлетворительно» - 2 «Хорошо» - 3 «Отлично» - 4-5
- осуществлять изучение и обобщение научно-технической литературы, составлять обзор по вопросам обеспечения информационной безопасности.	Практическое занятие 6-10 (за занятие максимально 5 баллов)	Модуль 2 0÷5 за каждое ПЗ «Неудовлетворительно» - 0-1 «Удовлетворительно» - 2 «Хорошо» - 3 «Отлично» - 4-5
Владеть:		
- навыками работы с нормативными и методическими материалами по вопросам применения средств защиты информации.	Практическое занятие 1-5 (за занятие максимально 5 баллов)	Модуль 1 0÷5 за каждое ПЗ «Неудовлетворительно» - 0-1 «Удовлетворительно» - 2 «Хорошо» - 3 «Отлично» - 4-5
- навыками работы со справочной и научно-технической литературой по вопросам обеспечения информационной безопасности.	Практическое занятие 6-10 (за занятие максимально 5 баллов)	Модуль 2 0÷5 за каждое ПЗ «Неудовлетворительно» - 0-1 «Удовлетворительно» - 2 «Хорошо» - 3 «Отлично» - 4-5
ОПК-9: Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности		
Знать:		
- национальные стандарты Российской Федерации в области криптографической защиты информации и сферы их применения;	Теоретический блок (контрольная работа 1)	Модуль 1 0÷25 «Неудовлетворительно» - 0-10 «Удовлетворительно» - 11-15

- основные математические методы и алгоритмы шифрования, расшифрования и дешифрования сообщений; - алгоритмы электронной (цифровой) подписи в телекоммуникационных системах.		«Хорошо» - 16-20 «Отлично» - 21-25
- основные виды средств криптографической защиты информации (СКЗИ), включая блочные и поточные системы шифрования, криптографические системы с открытым ключом, криптографические хеш-функции и криптографические протоколы; - принципы функционирования программных средств криптографической защиты информации.; - виды криптографических протоколов и их место в комплексной системе защиты информации;	Теоретический блок (контрольная работа 2)	Модуль 2 0÷25 «Неудовлетворительно» - 0-10 «Удовлетворительно» - 11-15 «Хорошо» - 16-20 «Отлично» - 21-25
Уметь:		
- анализировать угрозы безопасности информации в компьютерных сетях;	Практическое занятие 1 – 5 (за занятие максимально 5 баллов)	Модуль 1 0÷5 за каждое ПЗ «Неудовлетворительно» - 0-1 «Удовлетворительно» - 2 «Хорошо» - 3 «Отлично» - 4-5
- использовать криптографические протоколы, применяемые в компьютерных сетях.	Практическое занятие 6-10 (за занятие максимально 5 баллов)	Модуль 2 0÷5 за каждое ПЗ «Неудовлетворительно» - 0-1 «Удовлетворительно» - 2 «Хорошо» - 3 «Отлично» - 4-5
Владеть:		
- навыками установки программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации.	Практическое занятие 1-5 (за занятие максимально 5 баллов)	Модуль 1 0÷5 за каждое ПЗ «Неудовлетворительно» - 0-1 «Удовлетворительно» - 2 «Хорошо» - 3 «Отлично» - 4-5
- навыками анализа и оценки угроз информационной безопасности объекта информатизации.	Практическое занятие 6-10 (за занятие максимально 5 баллов)	Модуль 2 0÷5 за каждое ПЗ «Неудовлетворительно» - 0-1 «Удовлетворительно» - 2 «Хорошо» - 3 «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 компетенции, 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 8 лекционных занятий и 5 практических занятий. Знание лекционного материала оценивается по контрольной работе, состоящей из двух вопросов, максимальное количество баллов за контрольную работу составляет 25. За выполненное и защищенное практическое занятие обучающийся получает максимум по 5 баллов, максимально за 5 практических занятий обучающийся может набрать 25 баллов. Общее максимальное количество баллов за каждый модуль составляет 50 баллов.

Вопросы для контрольной работы (ОПК-8 , ОПК-9):

1. Основные определения криптографии: криптография, криптология, криптографические анализ и синтез, криптографическая система, криптографическая стойкость, ключ, криптографический протокол, атака на криптосистему, конфиденциальность, целостность, аутентификация, невозможность отказа, неотслеживаемость, анонимность, несвязываемость, алфавит, текст, шифрсистема, бесключевая и ключевая функции хеширования.
2. Основные определения по протоколам: протокол, цикл и шаг протокола, коммуникационный протокол, обеспечения безопасности, функция - сервис безопасности, криптографический протокол, нарушитель, противник.
3. Основные определения по алгебраическим основам: декартово произведение множеств, бинарное отношение, виды отношений, сравнимость по модулю, классы вычетов, отображение, свойства функций, группоид, полугруппа, группа, абелева группа, кольцо, поле, поле Галуа, изоморфизм, поле вычетов, поле остатков от деления на многочлен.
4. Свойства, характеризующие безопасность протоколов.
5. Виды криптографических протоколов.
6. Основные атаки на безопасность протоколов.
7. Примитивные и прикладные протоколы.
8. Понятие о криптографических протоколах. Полнота и корректность.
9. Схема электронной подписи. Надежность схемы электронной подписи.
10. Схема выработки электронной подписи Эль-Гамала.
11. Схема Шнорра.
12. Двусторонние и трехсторонние протоколы передачи ключей. Транспортный протокол Шамира.
13. Доверенная третья сторона: функции. Ключевая структура. Понятие производного ключа.
14. Базовый протокол выработки общего ключа Диффи-Хеллмана. Протокол со взаимной аутентификацией.
15. Стандарты на электронную (цифровую) подпись:
16. Цифровая подпись DSS,
17. Цифровая подпись ГОСТ Р34.10-94.
18. Цифровые подписи, основанные на симметричных криптосистемах.
19. Функции хеширования:ГОСТ Р34.11-94, MD5.

20. Функции хеширования: SHA.
21. Основные требования к электронной подписи.
22. Алгоритмы электронной подписи: электронная подпись на основе криптосистемы RSA,
23. Электронная подпись на основе шифра Эль-Гамала.
24. Анализ электронной цифровой подписи на основе криптосистемы Эль Гамала

Практическое занятие №1 Использование симметричных и асимметричных шифрсистем для построения криптографических протоколов. Примеры. Основные подходы к автоматизации анализа протоколов.

Контрольные вопросы ПЗ№1 (ОПК-8, ОПК-9):

1. Протокол, цикл и шаг протокола.
2. Коммуникационный протокол.
3. Протокол обеспечения безопасности.
4. Криптографический протокол.
5. Нарушитель, противник.
6. Свойства, характеризующие безопасность протоколов.
7. Основные атаки на безопасность протоколов.
8. Симметричные криптографические системы (СКС). Виды СКС.

Практическое занятие №2. Функции хеширования: ГОСТ Р34.11-94, MD5, SHA.

Контрольные вопросы ПЗ№2 (ОПК-8, ОПК-9):

1. Бесключевые функции хеширования. Алгоритм Меркля-Дамгарда.
2. Функция хеширования «Стрибог» (ГОСТ Р 34.11-2012).
3. Алгоритм криптографической губки. Функция хеширования SHA-3 (Кессак).
4. Ключевые функции хеширования. Функция НМАС.
5. Ключевые функции хеширования. Режим выработки имитовставки (СМАС).

Практическое занятие №3. Стандарты США и России электронной цифровой подписи.

Контрольные вопросы ПЗ№3 (ОПК-8, 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. Какие услуги предоставляет центр сертификации ключей на платной основе?
11. На каких условиях строятся отношения между центром сертификации и пользователями?
12. Можно ли передавать секретный ключ ЭП другим лицам на время отсутствия владельца ключа?

Практическое занятие №4. Протокол открытого распределения ключей Диффи-Хеллмана.

Контрольные вопросы ПЗ№4 (ОПК-9):

1. Протоколы установления подлинности.
2. Управление ключами. Этапы жизненного цикла ключей.
3. Задачи управления ключами, решаемые криптографическими средствами.
4. Централизованная выработка ключа.
5. Совместная выработка ключа.
6. Требования к секретному ключу. Алгоритм фон Неймана.
7. Распределение ключа при наличии доверенного центра.
8. Распределение секретного ключа без участия доверенного центра.
9. Протокол Диффи-Хэллмана и атака «Человек посередине». Противодействие этой атаке.
10. Бесключевой протокол Шамира и атака «Человек посередине»

Практическое занятие №5. Групповые протоколы. Протоколы разделения секрета и распределения ключей для телеконференции.

Контрольные вопросы ПЗ№5 (ОПК-9):

1. Понятие о разделении секрета.
2. (пД)-пороговая схема разделения секрета. Схема Шамира.
3. Группа доступа, структура доступа. Требования к ним.
4. Минимальная группа доступа.
5. Совершенная СРС (система разделения доступа), идеальная СРС.
6. Пороговые схемы разделения секрета.
7. Схема Шамира, ее совершенность и идеальность.
8. Схема Блэкли. Вопрос о ее совершенности и идеальности.

Модуль 2: (50 баллов):

Модуль содержит 9 лекционных занятий и 5 практических занятий. Знание лекционного материала оценивается по контрольной работе, состоящей из двух вопросов, максимальное количество баллов за контрольную работу составляет 25. За выполненное и защищенное практическое занятие максимум 5 баллов, максимально за 5 практических занятий обучающийся может набрать 25 баллов.. Общее максимальное количество баллов за модуль 2 составляет 50.

Вопросы для контрольной работы (ОПК-9):

1. Виды протоколов идентификации.
2. Протоколы идентификации, использующие пароли.
3. Протоколы идентификации, использующие технику «запрос-ответ». Случайные последовательности и метки времени.
4. Протоколы идентификации, использующие технику доказательства знания.
5. Протоколы с нулевым разглашением.
6. Протокол привязки к биту.
7. Игровые протоколы. Подбрасывание монеты по телефону.
8. Протоколы подписания контрактов.
9. Сертифицированная электронная почта.
10. Аргумент с нулевым разглашением.

11. Схема электронного голосования.
12. Блокчейн (blockchain).
13. Биткоин. Транзакции и BTC.
14. Особенности построения семейства протоколов IPsec.
15. Протоколы SSL/TLS и особенности их реализации.
16. Электронные платежи. Первая схема Чома.
17. Электронные платежи. Вторая схема Чома.
18. Проблемы арбитража в электронных платежах и законные затемненные подписи.
19. Электронные монеты. Схема Якоби.
20. Электронные монеты. Схема Брандса.
21. Блокчейн (blockchain).
22. Анализ структуры и принципов функционирования вычислительных сетей с позиции обеспечения информационной безопасности.
23. Угрозы информационно-программному обеспечению, характерные только для распределённой вычислительной среды.
24. Использование криптографических методов для защиты данных, циркулирующих в вычислительной сети.

Практическое занятие №6. Протоколы идентификации.

Контрольные вопросы ПЗ№6 (ОПК-9):

1. Базовые этапы построения системы комплексной защиты вычислительных систем.
2. Анализ моделей нарушителя;
3. Угрозы информационно-программному обеспечению.
4. Идентификация пользователей и установление их подлинности при доступе к компьютерным ресурсам.
5. Основные этапы доступа к ресурсам вычислительной системы; использование простого пароля; использование динамически изменяющегося пароля.
6. Взаимная проверка подлинности и другие случаи опознавания.
7. Способы разграничения доступа к компьютерным ресурсам; разграничение доступа по спискам.

Практическое занятие №7. Протоколы решения математических задач.

Контрольные вопросы ПЗ№7 (ОПК-9):

1. Базовые этапы построения системы комплексной защиты вычислительных систем.
2. Анализ моделей нарушителя;
3. Угрозы информационно-программному обеспечению.
4. Идентификация пользователей и установление их подлинности при доступе к компьютерным ресурсам.
5. Основные этапы доступа к ресурсам вычислительной системы; использование простого пароля; использование динамически изменяющегося пароля.
6. Взаимная проверка подлинности и другие случаи опознавания.
7. Способы разграничения доступа к компьютерным ресурсам; разграничение доступа по спискам.

Практическое занятие №8. Схемы электронного голосования.

1.3.2 Контрольные вопросы ПЗ№8 (ОПК-8, ОПК-9):

1. Базовые этапы построения системы комплексной защиты вычислительных систем.
2. Анализ моделей нарушителя;
3. Угрозы информационно-программному обеспечению.
4. Идентификация пользователей и установление их подлинности при доступе к компьютерным ресурсам.
5. Основные этапы доступа к ресурсам вычислительной системы; использование простого пароля; использование динамически изменяющегося пароля.
6. Взаимная проверка подлинности и другие случаи опознавания.
7. Способы разграничения доступа к компьютерным ресурсам; разграничение доступа по спискам.

Практическое занятие №9. Криптовалюты.

Контрольные вопросы ПЗ№9 (ОПК-8, ОПК-9):

1. Базовые этапы построения системы комплексной защиты вычислительных систем.
2. Анализ моделей нарушителя;
3. Угрозы информационно-программному обеспечению.
4. Идентификация пользователей и установление их подлинности при доступе к компьютерным ресурсам.
5. Основные этапы доступа к ресурсам вычислительной системы; использование простого пароля; использование динамически изменяющегося пароля.
6. Взаимная проверка подлинности и другие случаи опознавания.
7. Способы разграничения доступа к компьютерным ресурсам; разграничение доступа по спискам.

1.3.2. Вопросы, выносимые на зачет с оценкой по дисциплине «Криптографические протоколы» (ОПК-8, ОПК-9) (промежуточная аттестация):

1. Понятие о криптографических протоколах. Основные виды протоколов.
2. Прimitивные и прикладные протоколы.
3. Понятие о криптографических протоколах. Полнота и корректность.
4. Протоколы подбрасывания монеты. Применение протоколов подбрасывания монеты для выработки сеансовых ключей .
5. Связанность и секретность протокола электронной жеребьевки. Пример протокола с безусловной связанностью.
6. Протоколы привязки к биту. Блоб.
7. Понятие о разделении секрета. Группа доступа, структура доступа. Требования к ним. Минимальная группа доступа .
8. Совершенная СРС (система разделения доступа), идеальная СРС.
9. Пороговые схемы разделения секрета. Схема Шамира, ее совершенность и идеальность.
10. Схема Блэкли. Вопрос о ее совершенности и идеальности .
11. СРС на основе Китайской теоремы об остатках. Вопрос о ее совершенности и идеальности.

12. СРС для произвольной структуры доступа. Вопрос о ее совершенности и идеальности.
13. Протоколы конфиденциальных вычислений.
14. Проверяемое разделение секрета .
15. Протоколы идентификации. Классификация. Требования.
16. Парольные схемы. Разновидности. Область применения.
17. Интерактивные системы доказательств. Полнота, корректность.
18. Пример интерактивной системы доказательств для языка «Квадратичные невычеты».
19. Доказательства с нулевым разглашением. Статистическая неразличимость.
20. Вероятностная неразличимость. Пример интерактивного доказательства с нулевым разглашением для языка «Изоморфизм графов» .
21. Протоколы идентификации на основе теории ИСД с нулевым разглашением. Схема Фиата-Шамира. Схема Файге-Фиата-Шамира. Их полнота и корректность.
22. Схема идентификации Шнорра. Схема Брикелла-МакКарли. Их полнота и корректность .
23. Схема идентификации Окамото и теорема о ее условной стойкости.
24. Схема Гиллу-Кискатр. Ее полнота и корректность.
25. Слепая подпись .
26. Скрытый канал .
27. Протокол «Покер по телефону».
28. Электронная монета. Электронные деньги.
29. Требования к схемам электронных денег. Схема электронного кошелька с банкнотами одного достоинства.
30. Требования к схемам электронных денег разного достоинства. Схема с копилкой.
31. Протоколы голосования.
32. Протоколы установления подлинности.
33. Управление ключами. Этапы жизненного цикла ключей. Задачи управления ключами, решаемые криптографическими средствами.
34. Централизованная выработка ключа. Совместная выработка ключа. Требования к секретному ключу. Алгоритм фон Неймана.
35. Распределение ключа при наличии доверенного центра
36. Распределение секретного ключа без участия доверенного центра.
37. Схемы Wide -Mouth Frog, Yahalom. Их анализ.
38. Протокол Нидхема-Шредера. Его анализ.
39. Протокол Отвея-Рииса. Его анализ.
40. Бесключевой протокол Шамира и атака «Человек посередине».
41. Протокол Диффи-Хэллмана и атака «Человек посередине». Противодействие этой атаке.
42. Протокол Нидхема-Шредера на основе шифра с открытым ключом.
43. Широковещательное распределение ключей.
44. Инфраструктура открытых ключей. Сертификаты и справочники открытых ключей.

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 практическим занятиям для оценки практических навыков;
- промежуточная аттестация по дисциплине – в форме 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 обучающимся баллы могут быть переведены в оценку:

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

Для получения зачета обучающемуся достаточно набрать от 41 и более баллов.

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

Таблица 1 - Распределение баллов по блокам модулей дисциплины «Криптографические протоколы»

Модуль	Всего баллов (Максимальное значение)	Теоретический блок (Контрольная работа)	Практический блок (Распределение баллов по занятиям)
Модуль 1	50	25	25
Модуль 2	50	25	25
Зачет с оценкой	100	100	

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

На зачете с оценкой производится оценка тех компетенций, которые должны быть в той или иной форме освоены в процессе изучения. Рекомендуются формировать вопросы в

экзаменационных билетах таким образом, чтобы преподаватель смог оценить все компетенции данной дисциплины.

3 Промежуточная аттестация

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

Образец билета к зачету с оценкой.

	МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РФ 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: 4 Дисциплина: Криптографические протоколы		
Билет №1 1. Понятие о криптографических протоколах. Полнота и корректность. 2. Интерактивные системы доказательств. Полнота, корректность. Доцент, к.т.н. _____ Шухардин А.Н. «___» _____ 20__ г.		

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

4 Тестовые задания по дисциплине «Криптографические протоколы»

Тестовые задания позволяют оценить уровень сформированности компетенции ОПК-8 - Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности, а также компетенции ОПК-9 - Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности.

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

Базовый уровень (Блок А) 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 (Блок Б) в среднем составляет 35 % заданий.

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

Высокий уровень (Блок В) 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 компетенциям ОПК-8 и ОПК-9 равно 20.

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

ОПК-8 - Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности, а также компетенции ,

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	Дисциплина	Тексты заданий
1	Б1.О.36.02 Криптографические протоколы	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	Б1.О.36.02 Криптографические протоколы	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	Б1.О.36.02 Криптографические протоколы	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	Б1.О.36.02 Криптографические протоколы	Какой контроль относится к организационным? (один вариант) 1. Экран блокировки ОС. 2. Видео-наблюдение в серверной. 3. Регламент управления доступом и роли.

№ задания	Дисциплина	Тексты заданий
		4. Модуль TPM.
5	Б1.О.36.02 Криптографические протоколы	Что является типичным результатом анализа рисков? (один вариант) 1. План обработки рисков. 2. Схема адресного пространства сети. 3. Список MAC-адресов сотрудников. 4. Детальный отчет по нагрузочному тесту.
6	Б1.О.36.02 Криптографические протоколы	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	Б1.О.36.02 Криптографические протоколы	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	Б1.О.36.02 Криптографические протоколы	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	Б1.О.36.02 Криптографические протоколы	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	Б1.О.36.02 Криптографические протоколы	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	Дисциплина	Тексты заданий
11	Б1.О.36.02 Криптографические протоколы	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	Б1.О.36.02 Криптографические протоколы	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

№ задания	Дисциплина	Тексты заданий
		Г. АВАС
13	Б1.О.36.02 Криптографические протоколы	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 применение: А. Обнаружение и регистрация Б. Классификация и эскалация В. Ликвидация и восстановление Г. Последующий анализ
14	Б1.О.36.02 Криптографические протоколы	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	Дисциплина	Тексты заданий
15	Б1.О.36.02 Криптографические протоколы	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	Б1.О.36.02 Криптографические протоколы	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	Б1.О.36.02 Криптографические протоколы	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	Дисциплина	Тексты заданий
18	Б1.О.36.02 Криптографические протоколы	Вставьте термин: Документ, описывающий гипотетические возможности оппонента, его мотивацию, ресурсы и предполагаемые векторы атак — это ____.
19	Б1.О.36.02 Криптографические протоколы	Вставьте термин: Совокупность правил и требований к защите информации в организации, определяющая ответственность и принципы — это ____.
20	Б1.О.36.02 Криптографические протоколы	Вставьте термин: Процесс систематической оценки вероятности и последствий угроз для активов — это ____.

Система оценивания выполнения тестовых заданий по компетенции ОПК-8, формируемой дисциплиной «Криптографические протоколы»

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	Дисциплина	Тексты заданий
1	Б1.О.36.02 Криптографические протоколы	В каких единицах измеряется риск? 1. В стоимостном выражении 2. Во временном выражении 3. В процентах
2	Б1.О.36.02 Криптографические протоколы	Политика информационной безопасности необходима для: 1. Успешного прохождения компанией регулярного аудита по информационной безопасности 2. Обеспечения адекватной защиты наиболее важных ресурсов компании 3. Обеспечения реального уровня защищенности информационной системы компании
3	Б1.О.36.02 Криптографические протоколы	Международный стандарт управления информационной безопасностью ISO 17799 предъявляет: 1. Требования, предъявляемые только для узкого круга крупнейших мировых компаний 2. Базовые требования по обеспечению информационной безопасности 3. Требования, которые не соответствуют законам стран СНГ в области информационной безопасности
4	Б1.О.36.02 Криптографические протоколы	Для проведения анализа информационных рисков необходимо иметь: 1. Градацию информационных рисков 2. Полную модель информационной системы с точки зрения информационной безопасности 3. Вероятностные оценки угроз безопасности
5	Б1.О.36.02 Криптографические протоколы	Основной задачей теста на проникновение является: 1. Оценка возможности обнаружения атаки службой информационной безопасности компании 2. Проверка времени реакции службы обеспечения информационной безопасности 3. Оценка возможности осуществления атаки из Интернет на информационную систему компании
6	Б1.О.36.02 Криптографические протоколы	Тест на проникновение позволяет: 1. Убедить руководство компании в реальной опасности вторжения из Интернет и обосновать необходимость инвестиций в информационную безопасность 2. Снизить вероятные риски вирусной атаки на корпоративную сеть 3. Обеспечить должный уровень отношения руководства компании к проблеме обеспечения информационной безопасности
7	Б1.О.36.02 Криптографические протоколы	Одной из рекомендаций стандарта ISO 17799 является: 1. Четкая регламентация настроек межсетевых экранов 2. Применение антивирусных продуктов ведущих производителей 3. Проведение анализа рисков и регулярных тестов на проникновение сторонней компанией
8	Б1.О.36.02 Криптографические протоколы	Политика информационной безопасности в общем случае является: 1. Руководящим документом для администраторов безопасности и системных администраторов 2. Руководящим документом для всех сотрудников компании 3. Руководящим документом для руководства компании, менеджеров, администраторов безопасности и системных администраторов
9	Б1.О.36.02 Криптографические протоколы	Укажите в общем случае возможные типовые пути воздействия при получении удаленного доступа пользователя к информации на сервере 1. Атака на станцию пользователя, атака на канал передачи, атака на сервер 2. Вирусная атака на корпоративную сеть 3. Проникновение злоумышленника в сеть компании из Интернет
10	Б1.О.36.02	Какой метод обычно используется профессиональными взломщиками при

№ задания	Дисциплина	Тексты заданий
	Криптографические протоколы	информационной атаке? 1. Атака на наиболее защищенную цель 2. Атака на промежуточную цель 3. Атака осуществляется без целенаправленного выбора цели 4. Атака на наименее защищенную цель

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

№ задания	Дисциплина	Тексты заданий
11	Б1.О.36.02 Криптографические протоколы	Установите соответствие ключа доступа для проверки цифровой подписи под документом 1. Приватный 2. Открытый 3. Внутренний 4. Закрытый А. Ключ доступа, который считывается из внутренней памяти и является генерацией случайной последовательности Б. Набор уникальных символов без информации о владельце. Он нужен для создания электронной подписи и ее защиты от компрометации. В. Сертификат, который включает в себя все данные о владельце электронной подписи и удостоверяющем центре. Г. Длинная строка символов, которая действует как пароль, предоставляя доступ к криптовалютному аккаунту пользователя.
12	Б1.О.36.02 Криптографические протоколы	Установите соответствие алгоритма 1. Дискретное логарифмирование 2. Вычисление обратного элемента 3. Факторизации чисел 4. Нахождение большого простого числа А. Это алгоритм разложения в произведение простых множителей. Лежит в основе широко используемых алгоритмов, например, RSA. Б. Это алгоритм, который рассматривают в мультипликативной группе кольца вычетов или конечного поля, а также в группе точек эллиптической кривой над конечным полем. В. Это алгоритм нахождения числа, которое при умножении с исходным элементом даёт остаток 1 по заданному модулю (расширенный алгоритм Евклида) Г. Это алгоритм нахождения всех простых чисел не больше заданного числа (решето Эратосфена)
13	Б1.О.36.02 Криптографические протоколы	Установите соответствие научных дисциплин: 1. Защита информации 2. Криптография 3. Авторское право 4. Криптоанализ А. Это наука о методах дешифровки зашифрованной информации без предназначенного для этого ключа, а также сам процесс такой дешифровки Б. Это комплекс мероприятий, направленных на обеспечение информационной безопасности В. Это раздел гражданского права, который регулирует отношения, связанные с созданием и использованием произведений науки, литературы, искусства, а также программного обеспечения и баз данных. Г. Это наука о математических методах обеспечения конфиденциальности и аутентичности (целостности и подлинности авторства) информации
14	Б1.О.36.02 Криптографические протоколы	Установите соответствие направления информационной безопасности соответствующим мероприятиям 1. Правовая защита 2. Организационная защита 3. Инженерно-техническая защита А. Установка кодовых замков на дверях. Б. Разработка локальных нормативных актов.

№ задания	Дисциплина	Тексты заданий
		В. Подбор сотрудников для работы в службе информационной безопасности. Б, В, А

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

Инструкция: Прочитайте текст и установите правильную последовательность

№ задания	Дисциплина	Тексты заданий
15	Б1.О.36.02 Криптографические протоколы	Расставьте в порядке значимости нормативные акты, регламентирующие вопросы информационной безопасности: 1. Локальные нормативные акты; 2. Приказы соответствующих Министерств и Ведомств; 3. Законы РФ; 4. Указы Президента РФ; 5. Конституция РФ; 6. Постановления Правительства РФ.
16	Б1.О.36.02 Криптографические протоколы	Установите правильный порядок проведения анализа рисков информационной безопасности информационной системы: 1. Идентификация имеющихся угроз и уязвимостей безопасности, возможные осуществления угроз 2. Определение важности различных ресурсов для организации 3. Расчёт рисков, связанных с реализацией угроз безопасности. 4. Определение основных ресурсов информационной системы.
17	Б1.О.36.02 Криптографические протоколы	Расставьте порядок противодействия хакерской атаке: 1. Настройка средств защиты (необходимо применить правила на сетевых экранах и выполнить необходимые настройки на других системах защиты информации) 2. Устранение уязвимостей (нужно исправить уязвимости, которые привели к инциденту: установить обновления безопасности, удалить вредоносное ПО, сменить пароли и ключи доступа) 3. Локализация инцидента (необходимо заблокировать вредоносный трафик, изолировать заражённые системы от сети) 4. Анализ причин и превентивные меры

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

Инструкция: Прочитайте текст и запишите обоснованный ответ

№ задания	Дисциплина	Тексты заданий
18	Б1.О.36.02 Криптографические протоколы	Добавить недостающие слова в определение криптографии: Криптография — наука о математических _____ обеспечения _____, целостности данных, аутентификации и _____.
19	Б1.О.36.02 Криптографические протоколы	Добавить недостающие слова в определение шифрования информации: Шифрование информации — это процесс преобразования данных из открытого в зашифрованный вид с помощью специального математического _____ и _____.
20	Б1.О.36.02 Криптографические протоколы	Определить, что относится к конфиденциальности и аутентификации информации Процедура проверки подлинности, которая позволяет подтвердить личность пользователя или подлинность устройства при доступе к системе, сервису или данным. – это _____ Принципы и практика защиты данных от несанкционированного доступа, разглашения или использования информации – это _____

**Система оценивания выполнения тестовых заданий по компетенции ОПК-9,
формируемой дисциплиной «Криптографические протоколы»**

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 практических занятиях следует обратить внимание на соответствие выбираемых обучающимися средств решаемым в работе задачам.

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

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

2. Методические рекомендации обучающимся

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

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

2.1 Методические указания для обучающихся по лекционным занятиям

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

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

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

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

2.2 Методические указания для обучающихся по подготовке к практическим занятиям

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

При подготовке к практическому занятию целесообразно выполнить следующие рекомендации:

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

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

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

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

Для подготовки и выполнения практических занятий используется методическая разработка: Рыбалко И.П. Методические указания по проведению практических занятий по дисциплине «Основы криптографии»/ Рыбалко И.П. – Ростов-на -Дону: Изд-во СКФ МТУСИ, 2019. – 53 с.: ил.»

3. Методические рекомендации для обучающихся по самостоятельной работе

Самостоятельная работа обучающихся является составной частью учебной работы и имеет целью закрепление и углубление полученных знаний и навыков, поиск и приобретение новых знаний, в том числе с использованием автоматизированных обучающих курсов (систем), а также выполнение учебных заданий, подготовку к предстоящим занятиям, зачетам и экзаменам.

Самостоятельная работа во внеаудиторное время включает в себя:

- повторение лекционного материала;
- подготовки к лабораторным работам (практическим занятиям);
- изучения учебной и научной литературы;
- решения задач, выданных на практических занятиях;
- подготовки к тестированию;
- выделение наиболее сложных и проблемных вопросов по изучаемой теме, получение разъяснений и рекомендаций по данным вопросам с преподавателями кафедры на их еженедельных консультациях.

- проведение самоконтроля путем ответов на вопросы текущего контроля знаний, решения представленных в учебно-методических материалах кафедры задач, тестов, написания рефератов по отдельным вопросам изучаемой дисциплины.

Материал, подлежащий обработке на самостоятельных занятиях, намечается при разработке программы самостоятельной работы. Опыт, накопленный кафедрами в организации самостоятельных занятий, что материал, выделяемый на такие занятия, должен удовлетворять следующим требованиям:

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

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

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

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

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

Приветствуется использование компьютеров, которое:

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

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

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

Таблица – 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.	Час ов всег о: 36	Неделя
Модуль 1 – 18 часов			
1	Нормативно-правовые акты Российской Федерации о ведении электронного документооборота.	14	1-6
2	Федеральный закон Российской Федерации «Об электронной подписи» 6.04.2011г. № 63-ФЗ РФ.	4	7-8
Модуль 2 –18 часов			
3	Анализ моделей нарушителя; угрозы информационно-программному обеспечению вычислительных систем и их классификация.	8	9-12
4	Использование криптографических методов для защиты данных, циркулирующих в вычислительной сети	10	13-16

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