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

Утверждаю
Зам. директора по УВР
_____ Н.А. Андреева
«29» 04 2024 г.

Криптографические протоколы Б1.О.36.02

рабочая программа дисциплины

Кафедра: **Информационной безопасности**
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
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	4	144/8 сем
Контактная работа, в том числе (по семестрам, курсам):		72/8 сем
Лекции		36/8 сем
Лабораторных работ		
Практических занятий		36/8 сем
Семинаров		
Самостоятельная работа		72/8 сем
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 сем
Число экзаменов с разбивкой по семестрам (курсам)		

Программу составил:
Доцент кафедры ИТСС, к.т.н., доцент Шухардин А.Н.

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

Рабочая программа дисциплины
«Криптографические протоколы»

разработана в соответствии с ФГОС ВО:
направления подготовки 10.03.01 «Информационная безопасность», утвержденным приказом Министерства образования и науки 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 № 9 от 22.04.2024, и утвержденного директором СКФ МТУСИ 22.04.2024 г.

Рассмотрена и одобрена на заседании кафедры
«Информационная безопасность»

Протокол от «24» апреля 2024 г. № 9

Зав. кафедрой _____ Д.В. Маршаков

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР _____
-__ _____ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры
"Информационная безопасность"

Протокол от _ _____ 20__ г. № _
Зав. кафедрой _____

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР _____
-__ _____ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры

"Информационная безопасность"

Протокол от _ _____ 20__ г. № _
Зав. кафедрой _____

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР _____
-__ _____ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры
"Информационная безопасность"

Протокол от _ _____ 20__ г. № _
Зав. кафедрой _____

---

1. Цели изучения дисциплины

Целями изучения дисциплины **"Криптографические протоколы"** является формирование у обучаемых знаний в области существующих подходов к анализу и синтезу криптографических протоколов, с государственными и международными стандартами в этой области.

2. Планируемые результаты обучения

Изучение дисциплины направлено на формирование у выпускника способности решать профессиональные задачи в соответствии с ***организационно-управленческой деятельностью.***

Результатом освоения дисциплины являются сформированные у выпускника следующие компетенции:

Компетенции выпускника, формируемые в результате освоения дисциплины (в части, обеспечиваемой дисциплиной)
ОПК-1.2: способен администрировать средства защиты информации в компьютерных системах и сетях
Знать:
- принципы администрирования средства защиты информации в компьютерных сетях; - защищенные протоколы передачи данных в сети Интернет
Уметь:
- использовать средства администрирования компьютерных сетей и информационных систем.
Владеть:
- навыками настройки и управления конфигурацией устройств коммутации и маршрутизации, - навыками обеспечения безопасности веб-ресурсов.

3. Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Б1.О.29 Методы и средства криптографической защиты информации
2	Б1.О.32 Основы управления информационной безопасностью
3	Б1.О.36.06 Администрирование средств защиты информации в компьютерных системах и сетях
4	Б1.О.30 Программно-аппаратные средства защиты информации
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Б1.В.01 Обеспечение безопасности персональных данных в информационных системах
2	Б3.01 Подготовка к процедуре защиты и защита выпускной квалификационной работы

Рабочая программа дисциплины для инвалидов и лиц с ограниченными возможностями здоровья разрабатывается индивидуально с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

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					
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	Л1	2	ОПК-1.2	Л1.1 Л1.2
1.2	Лекция №2. Понятие уязвимости и атаки на криптографический протокол. Основные виды криптографических систем.	Л2	2	ОПК-1.2	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	2	ОПК-1.2	Л3.1
1.4	Лекция №3. КРИПТОГРАФИЧЕСКИЕ ХЕШ-ФУНКЦИИ. Хэш-функции MD-5, семейство SHA	Л3	2	ОПК-1.2	Л1.1 Л1.2
1.5	Практическое занятие № 2 Функции хеширования: ГОСТ Р34.11-94, MD5, SHA	ПЗ2	4	ОПК-1.2	Л3.1
1.6	Лекция № 4 СХЕМЫ ЦИФРОВОЙ ПОДПИСИ. Схемы цифровой подписи на основе симметричных и асимметричных шифрсистем. Схемы Эль-Гамаля, Нюберг-Рюппеля и Шнорра, их свойства Семейство схем типа ЭльГамаля.	Л4	4	ОПК-1.2	Л1.1 Л1.2
1.7	Лекция № 5 Одноразовые подписи. Схемы конфиденциальной цифровой подписи и подписи вслепую. Подписи с обнаружением подделки.	Л5	2	ОПК-1.2	Л1.1 Л1.2
1.8	Практическое занятие №3 Стандарты США и России электронной цифровой подписи.	ПЗ3	4	ОПК-1.2	Л3.1
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.	Л6	2	ОПК-1.2	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.	Л7	2	ОПК-1.2	Л1.1 Л1.2
1.8	Практическое занятие № 4 Протокол открытого распределения ключей Диффи-Хеллмана.	ПЗ4	4	ОПК-1.2	Л3.1
1.9	Лекция № 8. Групповые протоколы. Протоколы разделения секрета и распределения ключей для телеконференции.	Л8	2	ОПК-1.2	Л1.1 Л1.2
1.10	Практическое занятие № 5 Групповые протоколы. Протоколы разделения секрета и распределения ключей для телеконференции	ПЗ5	4	ОПК-1.2	Л3.1
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-1.2	Л1.1 Л1.2
Модуль 2 Прикладные криптографические протоколы					
2.1	Лекция №9. Протоколы идентификации. Протоколы идентификации на основе паролей, протоколы “рукопожатия” и типа «запрос-ответ»..	Л9	2	ОПК-1.2	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.	Л10	2	ОПК-1.2	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.	Л11	2	ОПК-1.2	Л1.1 Л1.2
2.4	Практическое занятие № 6 Протоколы идентификации.	ПЗ6	4	ОПК-1.2	Л3.1
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.	Л12	2	ОПК-1.2	Л1.1 Л1.2
2.6	Лекция № 13. Сертифицированная электронная почта. Аргумент с нулевым разглашением. Схемы электронного голосования.	Л13	2	ОПК-1.2	Л1.1 Л1.2
2.7	Практическое занятие №7 Протоколы решения математических задач.	ПЗ7	4	ОПК-1.2	Л3.1

2.8	Лекция № 14. Базовый протокол с нулевым разглашением (Жан-Жак Кискате (Jean-Jfcques Quisquater) и Луи Гилу (Louis Guillou)).	Л14	2	ОПК-1.2	
2.9	Практическое занятие № 8 Схемы электронного голосования	ПЗ8	2	ОПК-1.2	Л3.1
2.10	Лекция № 15. Особенности построения семейства протоколов IPsec	Л15	2	ОПК-1.2	Л1.1 Л1.2
2.11	Лекция № 16. Протоколы SSL/TLS и особенности их реализации.	Л16	2	ОПК-1.2	Л1.1 Л1.2
2.12	Практическое занятие № 9 Особенности построения семейства протоколов IPsec. Протоколы SSL/TLS и особенности их реализации.	ПЗ9	4	ОПК-1.2	Л3.1
2.13	Лекция № 17. Электронные платежи и электронные монеты. Крипто-валюты и блокчейн	Л17	2	ОПК-1.2	Л1.1 Л1.2
2.14	Практическое занятие № 10 Криптовалюты.	ПЗ 10	4	ОПК-1.2	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-1.2	Л1.1 Л1.2
Итого – 144 часа					

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Рекомендуемая литература

5.1.1. Основная литература

Код	Авторы, составители	Заглавие	Издатель-ство, год	Кол.
Л1.1	Лапонина О. Р.	Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия : учебное пособие / О. Р. Лапонина ; под редакцией В. А. Сухомлина. — 3-е изд. https://www.iprbookshop.ru/97571.html	М. : ИНТУИТ, Ай Пи Ар Медиа, 2020. — 605 с.	Э1
Л1.2	Баранова Е.К., Бабаш А.В.	Информационная безопасность и защита информации : учеб. пособие / — 3-е изд., перераб. и доп.	М. : РИОР : ИНФРА-М, 2017. — 322 с.	Э2

6.1.2. Дополнительная литература

Код	Авторы, составители	Заглавие	Издатель-ство, год	Кол.
Л2.1	Косолапов Ю. В.	Криптографические протоколы на основе линейных кодов : учебное пособие / Ю. В. Косолапов. https://www.iprbookshop .ru/100176 .html	Ростов-на-Дону, Таганрог : Изд-во ЮФУ, 2020. — 98 с.	Э3

Л2.2	Лось А.Б.	Криптографические методы защиты информации. Учебник для академического бакалавриата / А.Б. Лось, А.Ю. Нестеренко. М.И. Рожков - Режим доступа: http://znanium.com/catalog/product/474838	М.: Изд-во Юрайт, 2016.-476 с	Э4
6.1.3. Учебно-методическое обеспечение для самостоятельной работы обучающихся				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**
Л3.1	Шевчук П.С.	Методические указания по проведению практических занятий по дисциплине «Криптографические протоколы» / П.С. Шевчук. – Ростов-на - Дону: Изд-во СКФ МТУСИ, 2015. – 53 с.: ил.	РнД: СКФ МТУСИ, 2016	Э5
6.2. Электронные образовательные ресурсы				
Э1	https://www.iprbookshop.ru/97571 .html			
Э2	http://znanium.com/catalog/product/763644			
Э3	https://www.iprbookshop.ru/100176.html			
Э4	http://znanium.com/catalog/product/474838			
Э5	http://www.skf-mtusi.ru/?page_id=659			
6.3. Программное обеспечение				
П.1	Linux (свободное ПО)			
П.2	LibreOffice (свободное ПО)			
П.3	Kaspersky Endpoint Security (лицензия)			

6. Материально-техническое обеспечение дисциплины

6.1 МТО лекционных занятий	
1	Лекционная аудитория, оборудованная интерактивной доской, проектором
6.2 МТО лабораторных работ и практических занятий	
1	Компьютерные аудитории с возможностью выхода в локальную сеть Филиала и Интернет
6.3 МТО рубежных контролей, экзамена	
1	Компьютерные аудитории с возможностью выхода в локальную сеть Филиала и Интернет

7. Методические рекомендации для обучающихся по самостоятельной работе

Указания по подготовке к различным видам занятий

Подготовка к лекционным занятиям осуществляется систематически и сводится к повторению изученного материала и отработке тем, вынесенных на самостоятельную работу. При этом должен быть доработан конспект лекций, а также получены ответы на контрольные вопросы, которые, как правило, приводятся в конце каждого раздела учебных пособий. Особое внимание необходимо уделить пониманию изучаемого материала. Зафиксировать вопросы, которые следует задать преподавателю.

Подготовка к лабораторным и практическим занятиям должна проводиться в объеме тех указаний, которые приводятся в каждом методическом пособии для проведения соответствующего занятия. Тема очередного занятия объявляется преподавателем накануне.

После повторения лекционного материала необходимо ознакомиться с предлагаемыми практическими заданиями, уяснить их суть, продумать порядок их выполнения, уточнить достаточность своих знаний для выполнения задания. Целесообразно выполнить возможные заготовки из состава отчета, который предстоит оформить на занятии. Это позволит выполнить и защитить работу в период плановых часов. Перед проведением каждого занятия должно быть полное представление о сути и порядке выполнения предстоящей работы.

Существенное значение имеет самостоятельная работа студента.

Темы для самостоятельного изучения для различных форм обучения, информационные источники и рекомендуемое время указаны в Разделе 4 настоящей Рабочей программы.

Самостоятельная работа студентов по дисциплине проводится в течение всего семестра и складывается из нескольких составляющих.

Подготовка к плановым аудиторным занятиям. В начале семестра студентов знакомят с календарным планом проведения всех видов учебных занятий. Чтобы студенты могли проверить качество своей подготовки к занятиям, в учебных пособиях и методических указаниях к лабораторным работам имеются вопросы для проверки уровня знаний перед выполнением работы и контрольные вопросы, позволяющие студенту оценить качество полученных результатов после выполнения работы. Предлагаемые студентам учебные пособия кроме контрольных вопросов содержат примеры с решениями и упражнения по основным темам.

Изучение технической литературы. Студенты самостоятельно изучают рекомендованную преподавателем техническую литературу.

Дополнительные самостоятельные исследования в лаборатории. Студенты, желающие получить более глубокие знания, имеют возможность выполнить дополнительные самостоятельные исследования в лаборатории. С этой целью в плановых лабораторных работах предусмотрены возможности для дополнительных исследований. Перечень разделов программы, предлагаемых для самостоятельных исследований, доводится до сведения студентов в начале семестра.

Самостоятельная работа на ПЭВМ. Для повышения эффективности самостоятельной работы студентам во второй половине дня предоставляется возможность выполнить в лаборатории самостоятельные исследования с использованием программно-аппаратного комплекса, состоящего из виртуальных электронных приборов, отображаемых на экране ПЭВМ, и моделирующих программ. Исследуемые схемы могут собираться из реальных компонентов на лабораторном стенде или виртуальных компонентов, хранящихся в библиотеке ПЭВМ.

Источники, рекомендуемые для углубленного изучения учебного материала

1. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие. – М.: ДМК Пресс, 2011. – 416 с.;
2. Бирюков А.А. Информационная безопасность: защита и нападение. 2-е изд., перераб. и доп. – М.: ДМК Пресс, 2017. – 434 с.
3. Маршаков, Д. В. Программно-аппаратные средства защиты информации: учебное пособие / Д. В. Маршаков, Д. В. Фатхи. — Ростов-на-Дону: Донской ГТУ, 2021. — 228 с.
4. Воронов В.А., Тихонов В.А. Концептуальные основы создания и применения системы защиты объектов. – М.: Горячая линия - Телеком, 2013.
5. Хорев П.Б. Программно-аппаратная защита информации: учебное пособие. 3-е изд., испр. и доп. – Москва: ИНФРА-М, 2022. – 327 с.
6. Ерохин С.Д., Петухов А.Н., Пилюгин П.Л. Управление безопасностью критических информационных инфраструктур. – М.: Горячая линия – Телеком, 2021.
7. Климентьев, К. Е. Введение в защиту компьютерной информации: учебное пособие / К. Е. Климентьев. — Самара: Самарский университет, 2020. — 183 с.
8. Краковский, Ю. М. Методы защиты информации: учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург: Лань, 2021. — 236 с..
9. Никифоров, С. Н. Методы защиты информации. Пароли, скрытие, шифрование: учеб-ное пособие для вузов / С. Н. Никифоров. — 4-е изд., стер. — Санкт-Петербург: Лань, 2022. — 124 с.
10. Язов Ю.К., Соловьев С.В. Организация защиты информации в информационных системах от несанкционированного доступа: монография / Ю.К. Язов, С.В. Соловьев. – Воронеж: Кварта, 2018. – 588 с.
11. Профильные журналы «Электросвязь», «T-Comm: Телекоммуникации и транспорт» и другие.

Использование Интернет-ресурсов

1. Электронный ресурс https://www.securitylab.ru/
2. Электронный ресурс https://securelist.ru/
3. Электронный ресурс https://www.kaspersky.ru/
4. Электронный ресурс https://encyclopedia.kaspersky.ru/
5. Электронный ресурс https://www.drweb.ru/
6. Электронный ресурс http://infoprotect.net/category/news
7. Электронный ресурс https://www.it-world.ru/it-news/security/
8. Электронный ресурс https://threatpost.ru/
9. Электронный ресурс https://www.anti-malware.ru/

Рекомендации по подготовке к рубежным аттестациям

Подготовка к сдаче модуля сводится защите на дату проведения последнего занятия в рамках модуля всех практических и лабораторных занятий, а также к подготовке к ответам по тестовым заданиям.

Объем вопросов по каждому лабораторному и практическому занятию отражен в методических указаниях по проведению соответствующего занятия. Кроме того студент должен быть готов к пояснениям по сути практических приемов работы и доказыванию обоснованности принятых решений. Если работа не выполнена или не защищена своевременно, то это следует сделать в часы самоподготовки и консультаций до даты последнего занятия в рамках сдаваемого модуля.

Подготовка к выполнению теста обеспечивается изучением и повторением того материала, который изучался на лекционных занятиях и входе лабораторных и практических занятий. Материал повторяется по конспектам и учебным пособиям, указанным в списке литературы и методических указаниях.

Подготовка к зачету осуществляется на протяжении всего времени изучения дисциплины.

Для более конкретной, целенаправленной и качественной подготовки к зачету необходимо перед началом изучения дисциплины познакомиться с содержанием рабочей программы. Уяснить логику и последовательность изучения материала, уточнить конкретные конечные результаты, которые должны быть достигнуты в итоге изучения конкретных тем и занятий. Познакомиться с перечнем вопросов и заданий, выносимых на экзамен.

В ходе каждого занятия необходимо изучить все учебные вопросы и выполнить практические задания. Для оперативного оценивания уровня достижения учебных целей следует ответить на контрольные вопросы, которые имеются в руководстве для каждого практического и лабораторного занятия. В случае выявленных затруднений следует провести дополнительное изучение материала в часы самостоятельной работы или в период консультаций с преподавателем. Все учебные материалы должны быть отражены в конспекте, он должен дополняться и уточняться по мере отработки и уточнения учебных вопросов. Само ведение конспекта концентрирует внимание, упорядочивает знания, стимулирует активность в усвоении. К моменту выхода на непосредственную подготовку к зачету в конспекте не должно остаться непонятных вопросов.

В силу ограниченного времени, отводимого на непосредственную подготовку к зачету, целесообразно материал повторять в основном по отработанному конспекту. Это экономит время и дает возможность работать по уже знакомым записям, что улучшает запоминание материала. Остается спланировать работу в соответствии с имеющимся временем и жестко придерживаться намеченного плана. В период обязательных плановых предэкзаменационных консультаций необходимо уточнить организационные вопросы проведения экзамена и при необходимости - сложные вопросы по существу материала.

Дополнения и изменения в Рабочей программе