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
_____А.Г. Жуковский
«23» 05 2022 г.

Криптографические протоколы ФТД.01
рабочая программа дисциплины

Кафедра: Инфокоммуникационные технологии и системы связи
Направление подготовки: **11.03.02 Инфокоммуникационные технологии и системы связи**
Профиль: Защищенные системы и сети связи
Формы обучения: **очная, заочная**

Распределение часов дисциплины по семестрам (ОФ), курсам (ЗФ)

Вид учебной работы	ОФ		ЗФ	
	ЗЕ	часов	ЗЕ	часов
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	4	144/6	4	144/4
Контактная работа, в том числе (по семестрам, курсам):		32		36/4
Лекции		14/6		16/4
Лабораторных работ				
Практических занятий		18/6		20/4
Семинаров				
Самостоятельная работа		112/6		108/4
Контроль				
Число контрольных работ (по курсам)				
Число КР (по семестрам, курсам)				
Число КП (по семестрам, курсам)				
Число зачетов с разбивкой по семестрам (курсам)		1/6		1/4
Число экзаменов с разбивкой по семестрам (курсам)				

Программу составили:

Профессор кафедры Инфокоммуникационные технологии и системы связи д.т.н., профессор Шевчук П.С.

Рецензенты:
ведущий научный сотрудник ФГУП «Ростовский-на-Дону НИИ радиосвязи» ФНПЦ доктор технических наук А.В. Елисеев

Рабочая программа дисциплины
Криптографические протоколы

Разработана в соответствии с ФГОС ВО:
направления подготовки 11.03.02 ИНФОКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ И СИСТЕМЫ СВЯЗИ,
утвержденным приказом Министерства образования и науки Российской Федерации от 19 сентября 2017 г. № 930.

Составлена на основании учебных планов
направления 11.03.02 Инфокоммуникационные технологии и системы связи, профиля «Защищенные системы и сети связи»,
одобренных Учёным советом СКФ МТУСИ, протокол №7 от 28.02.2022г., и утвержденного директором СКФ МТУСИ 28.02.2022 г.

Одобрена на заседании кафедры «Инфокоммуникационные технологии и системы связи»

Протокол от 23.05. 2022 г. № 10
Зав. кафедрой _____ В.И. Юхнов

Визирование для использования в 201__/201__ уч. году

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

Протокол от __ __ 20__ г. № _

Зав. кафедрой _____ В.И. Юхнов

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

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

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 ИТСС

Протокол от _ _____ 20__ г. № _

Зав. кафедрой _____

---

1. Цели изучения дисциплины

Целью преподавания дисциплины является формирование у обучаемых знаний в области криптографических методов защиты информации и навыков практического обеспечения защиты информации и безопасного использования программных и аппаратных средств в сетях и системах связи.

2. Планируемые результаты обучения

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

Результатом освоения дисциплины являются сформированные у выпускника следующие компетенции:

Компетенции выпускника, формируемые в результате освоения дисциплины (в части, обеспечиваемой дисциплиной)
ПК-10: Способен обеспечить защиту от несанкционированного доступа сооружений и средств связи сетей электросвязи
Знать (Необходимые знания):
Основные математические методы и алгоритмы шифрования, расшифрования и дешифрования сообщений. Электронной (цифровой) подписи в телекоммуникационных системах. Принципы работы, структурные схемы, протоколы и способы программирования криптосистем и систем электронной подписи.
Уметь (Необходимые умения):
Определять опасности и угрозы, возникающие в развитии современного информационного общества. Пользоваться методами теории чисел. Составлять протоколы шифрования и расшифрования сообщений.
Владеть (Трудовые действия):
Языком предметной области: основными терминами, понятиями, определениями в области информационной безопасности Способностью сознавать опасности и угрозы, возникающие в развитии современного информационного общества Способностью сознавать опасности и угрозы, возникающие в развитии современного информационного общества, соблюдать основные требования информационной безопасности

3. Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Б1.О.25 «Основы информационной безопасности сетей и систем»
2	Б1.О.07 «Информатика»
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Б1.В.13 «Многоканальные цифровые системы передачи и средства их защиты »
2	Б1.В.ДВ.05.01 «Технические средства и методы защиты информации»

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 144 часа, 32 часов контактной работы)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компе-тенции	УМИО
Курс 3, Семестр 6					
Модуль 1 Протоколы и их классификация – 70 (14+56) часов					
1.1	Лекция 1. Понятие протокола, его отличие от алгоритма, основные характеристики протокола, задача криптографического протокола. Классификация криптографических протоколов по степени их развития. Действующие лица криптографических протоколов. Типы протоколов (классификация по способу реализации).	Лек 1.	2	ПК-10	Л1.1 Л1.3
1.2	Лекция 2. Симметричные и асимметричные КСЗИ. Основные требования к КСЗИ. Основные понятия криптографии: алфавит, открытый текст, закрытый текст (криптограмма), шифрование, расшифрование, секретный ключ. Криптоанализ и дешифрование.	Лек 2.	2	ПК-10	Л1.1 Л1.3
1.3	Лекция 3. Обмен ключами средствами симметричной криптографии. Базовый протокол. Протокол Нилхема-Шрёдера. Протокол Kerberos. Протокол Ньюмана-Стабблбайна..	Лек 3.	2	ПК-10	Л1.1 Л1.2 Л1.3
1.4	Практическое занятие №1 Криптоанализ и дешифрование. Правило Керкхоффса. Криптография и теория чисел. Модулярная арифметика.	ПЗ1.	4	ПК-10	Л1.1
1.5	Практическое занятие №2. Операторы шифрования: общие свойства и требования. Совершенная секретность и случайные ключи. Совершенный шифр Вернама. Информационная цена криптозащиты. Избыточность сообщений и её роль в криптоанализе. Оценка расстояния единственности.	ПЗ2	4	ПК-10	Л1.1
1.7	История появления шифров Схема Карнина – Грини – Хеллмана, на основе тео-рии матриц	СР	56	ПК-10	Л1.1
Модуль 2 Протоколы открытого распределения ключей – 74 (18+56) часов					
2.1	Лекция 4. Базовый протокол (алгоритм Диффи-Хеллмана). Алгоритм Диффи-Хеллмана с тремя и более участниками. Алгоритм Хьюза (Hughes). Протокол «станция-станция»	Лек 4.	4	ПК-10	Л1.2 Л2.1
2.2	Практическое занятие №3. Принципы блочного многораундового шиф-рования. Схема Фейстеля. Генерирование блочных шифров. Блочный шифр DES, разновидности алгоритма DES. Алгоритм RC6. Особенности отечественного стандарта шифрования ГОСТ 28147-89. Потоковые шифры. Примеры потоковых шифров.	ПЗ3	2	ПК-10	Л1.1 Л1.3
2.3	Практическое занятие №4. Основные этапы доступа к ресурсам вычислительной системы; использование простого пароля; использование динамически изменяющегося пароля; взаимная проверка подлинности и другие случаи опознания; способы	ПЗ4	2	ПК-10	Л1.1 Л1.3

	разграничения доступа к компьютерным ресурсам; разграничение доступа по спискам				
2.4	Лекция 5. Протоколы передачи секретного ключа по открытому каналу. Трехпроходный (трехэтапный) протокол Шамира. Алгоритм Шамира-Омура (Jim Omura). Формальные методы анализа протоколов.	Лек 5.	2	ПК-10	Л1.2 Л2.1
2.5	Лекция 6. Аутентификация при входе в систему. Аутентификация с помощью однонаправленных функций. Аутентификация средствами криптографии с открытым ключом. Взаимная аутентификация по протоколу взаимоблокировки.	Лек 6.	2	ПК-10	Л1.2
2.6	Практическое занятие №5. Базовые этапы построения системы комплексной защиты вычислительных систем; анализ моделей нарушителя; угрозы информационно-программному обеспечению вычислительных систем и их классификация	ПЗ №5	2	ПК-10	Л1.1 Л1.3
2.7	ПЗ №6 Функции хеширования: ГОСТ Р34.11-94, MD5, SHA	ПЗ6	2	ПК-10	Л1.2
2.8	Практическое занятие №7 Схемы аутентификации. Упрощенная схема идентификации Фейге-Фиата-Шамира. Схема идентификации Гиллу-Кискате. Протокол аутентификации Шнорра. Преобразование схем идентификации в схемы подписи. Схема подписи Фиата-Шамира. Схема подписи Гиллу-Кискате. Протокол цифровой подписи. Неоспоримая цифровая подпись Чаума (David Chaum). Подпись «вслепую». Подписи, подтверждаемые доверенным лицом	ПЗ7	2	ПК-10	Л2.1
2.9	Анализ структуры и принципов функционирования вычислительных сетей с позиции обеспечения информационной безопасности. Угрозы информационно-программному обеспечению, характерные только для распределённой вычислительной среды. Использование криптографических методов для защиты данных, циркулирующих в вычислительной сети.	СР	56	ПК-10	Л1.1 Л1.3
Итого – 144 часа					

4.2 Заочная форма обучения 5 лет (всего 144 часа, аудиторных 36 часов)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компе-тенции	УМИО
Курс 3, Семестр 6					
Модуль 1 Протоколы и их классификация – 70 (18+52) часов					
1.1	Лекция 1. Понятие протокола, его отличие от алгоритма, основные характеристики протокола, задача криптографического протокола. Классификация криптографических протоколов по	Лек 1.	4	ПК-10	Л1.1 Л1.3

	степени их раз-вития. Действующие лица криптографических протоколов. Типы протоколов (классификация по способу реализации).				
1.2	Лекция 2. Симметричные и асимметричные КСЗИ. Основные требования к КСЗИ. Основные понятия криптографии: алфавит, открытый текст, закрытый текст (криптограмма), шифрование, расшифрование, секретный ключ. Криптоанализ и дешифрование.	Лек 2.	4	ПК-10	Л1.1 Л1.3
1.3	Лекция 3. Обмен ключами средствами симметричной криптографии. Базовый протокол. Протокол Нилхема-Шрёдера. Протокол Kerberos. Протокол Ньюмана-Стабблбайна..	Лек 3.	2	ПК-10	Л1.1 Л1.2 Л1.3
1.4	Практическое занятие №1 Криптоанализ и дешифрование. Правило Керкхоффса. Криптография и теория чисел. Модулярная арифметика.	ПЗ1.	4	ПК-10	Л1.1
1.5	Практическое занятие №2. Операторы шифрования: общие свойства и требования. Совершенная секретность и случайные ключи. Совершенный шифр Вернама. Информационная цена криптозащиты. Избыточность сообщений и её роль в криптоанализе. Оценка расстояния единственности.	ПЗ2	4	ПК-10	Л1.1
1.7	История появления шифров Схема Карнина – Грини – Хеллмана, на основе теории матриц	СР	52	ПК-10	Л1.1
Модуль 2 Протоколы открытого распределения ключей – 74 (18+56) часов					
2.1	Лекция 4. Базовый протокол (алгоритм Диффи-Хеллмана). Алгоритм Диффи-Хеллмана с тремя и более участниками. Алгоритм Хьюза (Hughes). Протокол «станция-станция»	Лек 4.	2	ПК-10	Л1.2 Л2.1
2.2	Практическое занятие №3. Принципы блочного многораундового шиф-рования. Схема Фейстеля. Генерирование блочных шифров. Блочный шифр DES, разновидности алго-ритма DES. Алгоритм RC6. Особенности отечественного стандарта шифрования ГОСТ 28147-89. Потоковые шифры. Примеры потоковых шифров.	ПЗ3	4	ПК-10	Л1.1 Л1.3
2.3	Практическое занятие №4. Основные этапы доступа к ресурсам вычислительной системы; использование простого пароля; использование динамически изменяющегося пароля; взаимная проверка подлинности и другие случаи опознания; способы разграничения доступа к компьютерным ресурсам; разграничение доступа по спискам	ПЗ4	2	ПК-10	Л1.1 Л1.3
2.4	Лекция 5. Лекция 5. Протоколы передачи секретного ключа по открытому каналу. Трехпроходный (трехэтапный) протокол Шамира. Алгоритм Шамира-Омура (Jim Omura). Формальные методы анализа протоколов.	Лек 5.	2	ПК-10	Л1.2 Л2.1
2.5	Лекция 6. Аутентификация при входе в систему. Аутентификация с помощью однонаправленных функций. Аутентификация средствами криптографии с открытым ключом. Взаимная	Лек 6.	2	ПК-10	Л1.2

	аутентификация по протоколу взаимоблокировки..				
2.6	Практическое занятие №5. Базовые этапы построения системы комплексной защиты вычислительных систем; анализ моделей нарушителя; угрозы информационно-программному обеспечению вычислительных систем и их классификация	ПЗ №5	2	ПК-10	Л1.1 Л1.3
2.7	ПЗ №6 Функции хеширования: ГОСТ Р34.11-94, MD5, SHA	ПЗ6	2	ПК-10	Л1.2
2.8	Практическое занятие №7 Схемы аутентификации. Упрощенная схема идентификации Фейге-Фиата-Шамира. Схема идентификации Гиллу-Кискате. Протокол аутентификации Шнорра. Преобразование схем идентификации в схемы подписи. Схема подписи Фиата-Шамира. Схема подписи Гиллу-Кискате. Протокол цифровой подписи. Неоспоримая цифровая подпись Чаума (David Chaum). Подпись «вслепую». Подписи, подтверждаемые доверенным лицом	ПЗ7	2	ПК-10	Л2.1
2.9	Анализ структуры и принципов функционирования вычислительных сетей с позиции обеспечения информационной безопасности Угрозы информационно-программному обеспечению, характерные только для распределённой вычислительной среды Использование криптографических методов для защиты данных, циркулирующих в вычислительной сети	СР	56	ПК-10	Л1.1 Л1.3
Итого – 144 часа					

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Рекомендуемая литература				
5.1.1. Основная литература				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**
Л1.1	Бабаш А. В.	1. Криптографические методы защиты информации: Учебное пособие для вузов. http://znanium.com/catalog/product/1022055	М.: ИЦ РИОР, НИЦ ИНФРА-М, 2019. - 413 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
Л1.3	А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков;	Технические средства и методы защиты информации: Учебник для вузов / Под ред. А.П. Зайцева - 7 изд., исправ. - 60x90 1/16 - (Уч. для вузов). http://znanium.com/catalog/product/390284	М.: Гор. линия-Телеком, 2012. - 442с.	Э3
Л1.4	Скрыль С. В.	Технические средства и методы защиты информации / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. -.: ISBN 978-5-9912-0084-4 -	М.: Гор. линия-Телеком, 2012.	Э4

		Режим доступа: http://znanium.com/catalog/product/560580	- 616 с	
6.1.2. Дополнительная литература				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**
Л2.1	В.А. Ворона, В.А. Тихонов.	Инженерно-техническая и пожарная защита объектов -.: ил.; 60x90 1/16. - (Обеспечение безопасности объектов). ISBN 978-5-9912-0179-7, 1000 экз. - Режим доступа: http://znanium.com/catalog/product/344187	М.: Гор. линия-Телеком, 2012. - 512 с	Э5
Л2.2	А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин.	Защита информации: Учебное пособие - (Высшее образование: Бакалавриат; Магистратура). (переплет) ISBN 978-5-369-01378-6 - Режим доступа: http://znanium.com/catalog/product/474838	- М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с.:	Э6
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	Э7
Л3.2	Шевчук П.С..	Методические указания по проведению лабораторных работ по дисциплине «Криптографические протоколы»/ П.С. Шевчук. – Ростов-на -Дону: Изд-во СКФ МТУСИ, 2015. – 59 с.: ил.	РнД: СКФ МТУСИ, 2016	Э8
6.2. Электронные образовательные ресурсы				
Э1	http://znanium.com/catalog/product/1022055			
Э2	http://znanium.com/catalog/product/763644			
Э3	http://znanium.com/catalog/product/390284			
Э4	http://znanium.com/catalog/product/560580			
Э5	http://znanium.com/catalog/product/344187			
Э6	http://znanium.com/catalog/product/474838			
Э7	http://www.skf-mtusi.ru/?page_id=659			
Э8	http://www.skf-mtusi.ru/?page_id=659			
6.3. Программное обеспечение				
П.1	Python			
П.2	Scilab			
П.3	Word processor Microsoft Word or LibreOffice Writer.			

6. Материально-техническое обеспечение дисциплины

6.1 МТО лекционных занятий, ауд. 305	
1	Лекционная аудитория, оборудованная интерактивной доской, проектором
6.2 Аудитория 305 МТО лабораторных работ и практических занятий	
1	Компьютерная аудитория 305.
6.3 МТО рубежных контролей, экзамена	
1	Компьютерная аудитория 305

7. Методические рекомендации для обучающихся по самостоятельной работе

Самостоятельная работа студентов 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.

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

Методику самостоятельной работы все обучаемые выбирают индивидуально. Для более углубленного изучения материала по дисциплине целесообразно использовать учебные курсы сайта http://www.intuit.ru/ .

Для подготовки к рубежной аттестации и к экзамену целесообразно использовать материалы сайта http://i-exam.ru/ в режимах: «Тестирование обучение» и «Тестирование-самоконтроль». Студентам, успешно решающим тестовые задания целесообразно проверить свои силы, решая олимпиадные задания по информатике по адресу http://test.i-exam.ru/training/olymp/index.html .

Студентам очной формы обучения при освоении вопросов для самостоятельного изучения, представленных в подразделе 4.1, рекомендуется соблюдать последовательность их изучения, представленную в таблице 3.

Таблица 3 – Учебный материал, выносимый на самостоятельное изучение студентам очной формы обучения

№	Темы, разделы, вынесенные на самостоятельную подготовку, вопросы для подготовки к практическим и лабораторным занятиям; курсовые работы, содержание контрольных работ; рекомендации по использованию литературы, ЭВМ и др.	Часов всего: 112	Неделя
Модуль 1			
1	История появления шифров	19	1-2
2	Основные этапы жизненного цикла вирусов; объекты внедрения, режимы функционирования и специальные функции вирусов	19	3-4
3	Схемы заражения файлов; схемы заражения загрузчиков; способы маркировки, используемые вирусами	18	5-7
Модуль 2			
4	Анализ структуры и принципов функционирования вычислительных сетей с позиции обеспечения информационной безопасности	9	7-8
5	Угрозы информационно-программному обеспечению, характерные только для распределённой вычислительной среды	9	8-10
6	Использование криптографических методов для защиты данных, циркулирующих в вычислительной сети	9	10-138
7	Методы средства ограничения доступа к компонентам ЭВМ	9	14
8	Надёжность средств защиты компонент; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям	10	15
9	Методы средства хранения ключевой информации, типовые решения в организации ключевых систем; защита программ от излучения, способы встраивания средств защиты в программное обеспечение.	10	16-17

Студенты заочной формы обучения могут осваивать вопросы для самостоятельного изучения, представленные в подразделе 4.2 в произвольной последовательности, в удобное для них время. Однако к началу сессии они должны ориентироваться в материале, представленном в строках 1.2, 1.3, 1.6, 1.8, 2.2, 2.3, 2.5-2.7, 2.9, 2.10, 3.1 таблицы подраздела 4.2.

Дополнения и изменения