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
«30» 08 2021 г.

Основы криптографии Б1.В.ДВ.10.01
рабочая программа дисциплины

Кафедра: **Инфокоммуникационные технологии и системы связи**
Направление подготовки: **09.03.01 Информатика и вычислительная техника**

Профиль: Вычислительные машины, комплексы, системы и сети
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):	3	108/7	3	108/4
Контактная работа, в том числе (по семестрам, курсам):		64		10/4
Лекции		32/7		6/4
Лабораторных работ		16/7		
Практических занятий		16/7		4/4
Семинаров				
Самостоятельная работа		44/7		98/4
Контроль				
Число контрольных работ (по курсам)				
Число КР (по семестрам, курсам)				
Число КП (по семестрам, курсам)				
Число зачетов с разбивкой по семестрам (курсам)		1/7		1/4
Число экзаменов с разбивкой по семестрам (курсам)				

Программу составил:

Доцент кафедры ИТСС, к.т.н. Шухардин А.Н.

Рецензенты:
Заведующий кафедрой ИВТ, д.т.н. профессор Соколов С.В.

Рабочая программа дисциплины
«Основы криптографии»

Разработана в соответствии с ФГОС ВО:
направления подготовки 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА, утверждённым приказом Министерства образования и науки Российской Федерации от 19 сентября 2017 г. № 929.

Составлена на основании учебных планов
направления 09.03.01 Информатика и вычислительная техника,
профиля «Вычислительные машины, комплексы, системы и сети», одобренных Учёным советом СКФ МТУСИ, протокол №1 от 30.08.2021, и утвержденного директором СКФ МТУСИ 30.08.2021 г.

Рассмотрена и одобрена на заседании кафедры
Инфокоммуникационные технологии и системы связи

Протокол от 30. 08. 2021 г. № 1

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 _____ 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 ***проектной деятельностью.***

Результатом освоения дисциплины являются сформированные у выпускника следующие компетенции:

Компетенции выпускника, формируемые в результате освоения дисциплины (в части, обеспечиваемой дисциплиной)
ПК-1: Способен производить разработку и отладку программного кода, интегрировать программные модули и компоненты, проектировать программное обеспечение
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.18 «Основы информационной безопасности»
2	Б1.О.05 «Информатика»
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Б2.О.03(Пд) Производственная (проектно-технологическая) практика

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 108 часов, 64 часса контактной работы)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компе-тенции	УМИО
Курс 3, Семестр 6					
Модуль 1 Введение в криптографические системы защиты информации (КСЗИ) – 56 (34+22) часов					
1.1	Лекция 1. Информация как главный ресурс научно-технического и социально-экономического развития общества. Задачи обеспечения информационной безопасности телекоммуникационных систем. Система передачи информации с шифрованием сообщений. Три исторических этапа развития КСЗИ.	Лек 1	4	ПК-1	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	6	ПК-1	Л1.1 Л1.3
1.3	Лекция 3. Теоретико-информационные основы криптозащиты сообщений Количественные меры информации. Взаимная информация между криптограммой и ключом (первая криптотеорема Шеннона). Теоретическая стойкость КСЗИ.	Лек 3	6	ПК-1	Л1.1 Л1.2 Л1.3
1.4	Практическое занятие №1 Шифр столбцовой перестановки.	ПЗ 1	6	ПК-1	Л1.1
1.5	Практическое занятие №2. Шифр двойной перестановки.	ПЗ 2	6	ПК-1	Л1.1
1.6	Лабораторная работа №1. Шифры замены.	ЛР 1	6	ПК-1	
1.7	История появления шифров Основные этапы жизненного цикла вирусов; объекты внедрения, режимы функционирования и специальные функции вирусов. Схемы заражения файлов; схемы заражения загрузчиков; способы маркировки, используемые вирусами.	СР	22	ПК-1	Л1.1 Л1.3
Модуль 2 Симметричные КСЗИ Асимметричные КСЗИ – 52 (30+22) часов					
2.1	Лекция 4. Организация секретной связи с закрытым каналом передачи секретного ключа. Основные классы симметричных КСЗИ.	Лек 4	6	ПК-1	Л1.2 Л2.1
2.2	Лабораторная работа № 2. Шифры перестановки.	ЛР 2	4	ПК-1	Л1.1 Л1.3
2.3	Лабораторная работа № 3. Аддитивные шифры.	ЛР 3	2	ПК-1	Л1.1 Л1.3
2.4	Лекция 5. Современная криптография с открытыми ключами.	Лек 5	6	ПК-1	Л1.2 Л2.1
2.5	Лекция 6. Организация секретной связи без использования закрытого канала передачи секретного ключа. Примеры асимметричных алгоритмов шифрования и расшифрования.	Лек 6	4	ПК-1	Л1.2
2.6	Практическое занятие №3.	ПЗ 3	4	ПК-1	Л1.1

	Шифр простой замены.				Л1.3
2.7	Лабораторная работа № 4 Комбинированные шифры.	ЛР 4	2	ПК-1	Л1.2
2.8	Лабораторная работа № 5 Шифрование с открытым ключём.	ЛР 5	2	ПК-1	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	22	ПК-1	Л1.1 Л1.3
Зачёт					
Итого – 108 часов					

4.2 Заочная форма обучения 5 лет (всего 108 часов, аудиторных 10 часов)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
4 Курс, 8 семестр					
Модуль 1 Введение в криптографические системы защиты информации (КСЗИ) – 56 (2+54) часов					
1.1	Лекция 1. Информация как главный ресурс научно-технического и социально-экономического развития общества. Задачи обеспечения информационной безопасности телекоммуникационных систем. Система передачи информации с шифрованием сообщений. Три исторических этапа развития КСЗИ.	Лек 1	2	ПК-1	Л1.1 Л1.3
1.2	Симметричные и асимметричные КСЗИ. Основные требования к КСЗИ. Основные понятия криптографии: алфавит, открытый текст, закрытый текст (криптограмма), шифрование, расшифрование, секретный ключ. Криптоанализ и дешифрование.	СР	4	ПК-1	Л1.1 Л1.3
1.3	Теоретико-информационные основы криптозащиты сообщений Количественные меры информации. Взаимная информация между криптограммой и ключом (первая криптотеорема Шеннона). Теоретическая стойкость КСЗИ.	СР	4	ПК-1	Л1.1 Л1.3
1.4	Криптоанализ и дешифрование. Правило Керкхоффса. Криптография и теория чисел. Модулярная арифметика. 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. История появления шифров Основные этапы жизненного цикла вирусов; объек-	СР	46	ПК-1	Л1.1 Л1.2 Л1.3

	ты внедрения, режимы функционирования и специальные функции вирусов Схемы заражения файлов; схемы заражения загрузчиков; способы маркировки, используемые вирусами.				
Модуль 2 Симметричные КСЗИ Асимметричные КСЗИ – 52 (8+44) часов					
2.1	Лекция 2. Организация секретной связи с закрытым каналом передачи секретного ключа. Основные классы симметричных КСЗИ.	Лек 2	4	ПК-1	Л1.2 Л2.1
2.2	Практическое занятие №1. Шифр столбцовой перестановки.	ПЗ 1	4	ПК-1	Л1.1
2.3	Принципы блочного многораундового шифрования. Схема Фейстеля. Генерирование блочных шифров. Блочный шифр DES, разновидности алгоритма DES. Алгоритм RC6. Особенности отечественного стан дарта шифрования ГОСТ 28147-89. Потоковые шифры. Примеры потоковых шифров. Современная криптография с открытыми ключами. Организация секретной связи без использования закрытого канала передачи секретного ключа. Односторонние функции и функции-ловушки. Примеры асимметричных алгоритмов шифрования и расшифрования. Базовые этапы построения системы комплексной защиты вычислительных систем; анализ моделей нарушителя; угрозы информационно-программному обеспечению вычислительных систем и их классификация. Идентификация пользователей и установление их подлинности при доступе к компьютерным ресурсам. 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. 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. 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	44	ПК-1	Л1.1 Л1.2 Л2.1 Л1.1
Зачёт					
Итого – 108 часов					

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Рекомендуемая литература				
5.1.1. Основная литература				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**
Л1.1	Бабаш А. В.	Криптографические методы защиты информации: Учебное пособие для вузов.	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	Зайцев А.П., Шелупанов А.А., Мещеряков Р.В.	Технические средства и методы защиты информации: Учебник для вузов / Под ред. А.П. Зайцева - 7 изд., исправ .01/16 - (Уч. для вузов).	М.: Гор. линия-Телеком, 2012. - 442с.	Э3
Л1.4	Скрыль С. В., Зайцев А.П., Шелупанов А.А., Мещеряков Р.В.	Технические средства и методы защиты информации. Учебное пособие для ВУЗов.	М.:Гор. линия-Телеком, 2012. - 616 с	Э4
5.1.2. Дополнительная литература				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**
Л2.1	Ворона В.А., Тихонов В.А.	Инженерно-техническая и пожарная защита объектов (Обеспечение безопасности объектов).	М.: Гор. линия-Телеком, 2012. - 512 с	Э5
Л2.2	Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И.	Защита информации: Учебное пособие - (Высшее образование: Бакалавриат; Магистратура).	- М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с.:	Э6
5.1.3. Учебно-методическое обеспечение для самостоятельной работы обучающихся				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**
Л3.1	Рыбалко И.П.	Методические указания по проведению практических занятий по дисциплине «Основы криптографии»/ Рыбалко И.П. – Ростов-на -Дону: Изд-во СКФ МТУСИ, 2019. – 49 с.: ил.	РнД: СКФ МТУСИ, 2019	Э7
Л3.2	Рыбалко И.П.	Методические указания по проведению лабораторных работ по дисциплине «Основы криптографии»/– Ростов-на -Дону: Изд-во СКФ МТУСИ, 2019. – 59 с.: ил.	РнД: СКФ МТУСИ, 2019	Э8
5.2. 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			
5.3. 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	
1	Лекционная аудитория, оборудованная интерактивной доской, проектором.
6.2 МТО лабораторных работ и практических занятий	
1	Класс ПЭВМ, работающий под операционной системой не ниже WINDOWS XP.
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

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 занятии, предшествующему данному.

Методику самостоятельной работы все обучаемые выбирают индивидуально.

Студентам очной формы обучения при освоении вопросов для самостоятельного изучения, представленных в подразделе 4.1, рекомендуется соблюдать последовательность их изучения, представленную в таблице 1.

Таблица 1 – 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: 44	Неделя
Модуль 1			
1	История появления шифров	7	1-2
2	Основные этапы жизненного цикла вирусов; объекты внедрения, режимы функционирования и специальные функции вирусов	7	3-4
3	Схемы заражения файлов; схемы заражения загрузчиков; способы маркировки, используемые вирусами	8	5-7
Модуль 2			
4	Анализ структуры и принципов функционирования вычислительных сетей с позиции обеспечения информационной безопасности	3	7-8
5	Угрозы информационно-программному обеспечению, характерные только для распределённой вычислительной среды	3	8-10
6	Использование криптографических методов для защиты данных, циркулирующих в вычислительной сети	4	10-13
7	Методы средства ограничения доступа к компонентам ЭВМ	4	14

8	Надёжность средств защиты компонент; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям	4	15
9	Методы средства хранения ключевой информации, типовые решения в организации ключевых систем; защита программ от излучения, способы встраивания средств защиты в программное обеспечение.	4	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.

Дополнения и изменения