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.

Методы и средства криптографической защиты информации Б1.О.29

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):	5	180/5 сем
Контактная работа, в том числе (по семестрам, курсам):		86/5 сем
Лекции		34/5 сем
Лабораторных работ		34/5 сем
Практических занятий		18/5 сем
Семинаров		
Самостоятельная работа		58/5 сем
Контроль		36/5 сем
Число контрольных работ (по курсам)		
Число КР (по семестрам, курсам)		1/5 сем
Число КП (по семестрам, курсам)		
Число зачетов с оценкой с разбивкой по семестрам (курсам)		
Число экзаменов с разбивкой по семестрам (курсам)		1/5 сем

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
«Методы и средства криптографической защиты информации»

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 ***"Методы и средства криптографической защиты информации"*** являются формирование у обучаемых знаний в области принципов криптографических преобразований, типовых программно-аппаратных средств криптографической защиты информации и инфокоммуникаций от несанкционированного доступа.

2. Планируемые результаты обучения

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

Результатом освоения дисциплины являются сформированные у выпускника следующие компетенции:

Компетенции выпускника, формируемые в результате освоения дисциплины (в части, обеспечиваемой дисциплиной)
ОПК-9: способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности
Знать:
- основные математические методы и алгоритмы шифрования, расшифрования и дешифрования сообщений; - классификацию методов криптографического преобразования информации; - принципы функционирования программных средств криптографической 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; - национальные стандарты Российской Федерации в области криптографической защиты информации и сферы их применения; - алгоритмы электронной (цифровой) подписи в телекоммуникационных системах.
Уметь:
- пользоваться методами теории чисел - классифицировать и оценивать угрозы информационной безопасности; - использовать СКЗИ в автоматизированных системах; - использовать механизмы идентификации и аутентификации
Владеть:
- навыками анализа и оценки угроз информационной безопасности объекта информатизации; - навыками работы по основам защиты информации с использованием программно-аппаратных комплексов

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.06 Высшая математика
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Б1.О.36.02 Криптографические протоколы
2	Б1.В.02 Стеганографические методы скрытия информации
3	Б1.О.30 Программно-аппаратные средства защиты информации
4	Б1.О.33 Комплексное обеспечение защиты информации объекта информатизации

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 180 часов, 86 аудиторных часов, 58 часов самостоятельной работы)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
Курс 3, Семестр 5					
Модуль 1. Методы модулярной арифметики и аналитических преобразований.					
1.1	Лекция 1. ИНФОРМАЦИЯ КАК ГЛАВНЫЙ РЕСУРС НАУЧНО-ТЕХНИЧЕСКОГО И СОЦИАЛЬНО-ЭКОНОМИЧЕСКОГО РАЗВИТИЯ ОБЩЕСТВА. 1. Задачи обеспечения информационной безопасности телекоммуникационных систем. 2. Система передачи информации с шифрованием сообщений. 3. Три исторических этапа развития КСЗИ.	Л1	2	ОПК-9	Л1.1 Л1.2 Л1.3
1.2	Лекция 2. ОСНОВНЫЕ ТРЕБОВАНИЯ К КСЗИ. Основные понятия криптографии: алфавит, открытый текст, закрытый текст (криптограмма), шифрование, расшифрование, секретный ключ. Криптоанализ и дешифрование.	Л2	2	ОПК-9	Л1.1 Л1.2 Л1.3
1.3	Лекция 3. ТЕОРЕТИКО-ИНФОРМАЦИОННЫЕ ОСНОВЫ КРИПТОЗАЩИТЫ СООБЩЕНИЙ. 1 Количественные меры информации. 2. Взаимная информация между криптограммой и ключом (первая криптотеорема Шеннона). 3 Теоретическая стойкость КСЗИ.	Л3	2	ОПК-9	Л1.1 Л1.2 Л1.3
1.4	Лекция 4. МОДУЛЯРНАЯ АРИФМЕТИКА 1. Вычеты по модулю m. Теорема Эвклида 2. Свойство коммутативности . Функция Эйлера. 3. Свойства целочисленных операций mod N. 4. Вычисление обратных величин	Л4	4	ОПК-9	Л1.1 Л1.2 Л1.3
1.5	Практическое занятие 1. Вычисления по модулю n.	ПЗ1	2	ОПК-9	Л3.1
1.6	Практическое занятие №2 Общие формулы вычисления больших степеней	ПЗ2	2	ОПК-9	Л3.1
1.7	Лекция №5 КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ. Методы перестановки. Методы подстановки и замены. Методы аналитических преобразований	Л5	2	ОПК-9	Л1.1 Л1.2 Л1.3
1.8	Практическое занятие № 3 Методы умножения матриц, «укладки ранца».	ПЗ3	2	ОПК-9	Л3.1
1.9	Практическое занятие № 4 Метод полиномов.	ПЗ4	2	ОПК-9	Л3.1

1.10	Лабораторная работа №1. Шифры замены.	ЛР1	4	ОПК-9	Л3.2
1.11	Лабораторная работа №2. Шифры перестановки.	ЛР2	4	ОПК-9	Л3.2
1.12	Лекция №6. Гаммирование. Основные понятия. Методы тестирования псевдослучайных последовательностей . Комбинированные методы шифрования	Л6	4	ОПК-9	Л1.1 Л1.2 Л1.3
1.13	Практическое занятие № 5 Графические тесты. Проверка на монотонность. Оценочные тесты	ПЗ5	2	ОПК-9	Л3.1
1.14	Лабораторная работа № 3 Генерация дискретных случайных величин (событий) с помощью датчика ПСП.	ЛР3	4	ОПК-9	Л3.1
1.9	История появления шифров. Доктрина информационной безопасности Российской Федерации. Обеспечение сохранения коммерческой тайны предприятия. Каталог обобщенных мероприятий по защите конфиденциальной информации. Подходы к оценке стойкости алгоритмов шифрования. Электронные ресурсы модулярной арифметики. Калькуляторы. Псевдослучайные последовательности. Свойства, разновидности.	СРС	12	ОПК-9	Л1.1 Л1.2 Л1.3
Модуль 2 Криптографические системы защиты информации					
2.1	Лекция №7. СИММЕТРИЧНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ. 1. Схема Фейстеля. Типичные операции. Достоинства и недостатки. 2. Алгоритм DES. Режим шифрования. Алгоритм AES 3. Стандарт шифрования данных ГОСТ 34.12-2018. Алгоритм. Основные режимы шифрования. Основной шаг криптопреобразования.	Л7	4	ОПК-9	Л1.1 Л1.2 Л1.3
2.2	Практическое занятие №6 Режимы гаммирования и гаммирования с обратной связью	ПЗ6	2	ОПК-9	Л3.1
2.3	Лабораторная работа № 4 Блочный шифр DES, разновидности алгоритма DES.	ЛР4	4	ОПК-9	Л3.2
2.4	Лабораторная работа № 5 Алгоритм ГОСТ 34.12-2018.	ЛР5	4	ОПК-9	Л3.2
2.5	Лекция №8 АССИМЕТРИЧНЫЕ КРИПТОСИСТЕМЫ 1. Обобщенная схема асимметричной криптосистемы шифрования. 2. Характерные особенности асимметричных криптосистем.	Л8	4	ОПК-9	Л1.1 Л1.2 Л1.3
2.6	Лекция №9 АСИММЕТРИЧНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ 1. Алгоритм рюкзака. 2. Схемы шифрования RSA и Эль Гамаля. 3. Процедуры шифрования и дешифрования.	Л9	4	ОПК-9	Л1.1 Л1.2 Л1.3

	4. Гибридные схемы шифрования				
2.7	Практическое занятие №7 Криптоалгоритмы RSA и Эль Гамаля	ПЗ7	2	ОПК-9	Л3.1
2.8	Лабораторная работа № 6 Криптоалгоритм RSA	ЛР6	4	ОПК-9	Л3.2
2.9	Лекция №10 АЛГОРИТМЫ ХЭШИРОВАНИЯ 1. Криптографические хэш-функции. 2. Конструкция Меркла-Дамгарда . 3. Сравнительный анализ известных функций хэширования. 4. Функция ГОСТЗ 34.11-2018	Л10	2	ОПК-9	Л1.1 Л1.2 Л1.3
2.10	Практическое занятие №8 ТРЕБОВАНИЯ К ХЭШ-ФУНКЦИЯМ. СВОЙСТВА.	ПЗ8	2	ОПК-9	Л3.1
2.11	Лабораторная работа № 7 АЛГОРИТМЫ ХЭШИРОВАНИЯ	ЛР7	2	ОПК-9	Л3.2
2.12	Лекция №11 АЛГОРИТМЫ ЭЛЕКТРОННОЙ ПОДПИСИ (ЭП) 1. Электронная я подпись. Назначение и классификация. 2. Алгоритмы электронной цифровой подписи RSA и Эль Гамаля (EGSA). 3. Стандарт ГОСТ З 34.10-2018	Л11	4	ОПК-9	Л1.1 Л1.2 Л1.3
2.13	Практическое занятие №9 Процедура формирования и проверки ЭЦП	ПЗ9	2	ОПК-9	Л3.1
2.14	Лабораторная работа № 8 Стандарты на электронную (цифровую) подпись: цифровая подпись DSS, цифровая подпись ГОСТ Р34.10-2018. Цифровые подписи, основанные на симметричных криптосистемах.	ЛР8	4	ОПК-9	Л3.2
2.15	Лабораторная работа № 9 «Анализ электронной цифровой подписи на основе криптосистемы Эль Гамаля».	ЛР9	4	ОПК-9	Л3.2
2.16	Алгоритм симметричной системы шифрования данных – стандарт ГОСТ 34.12-2018. Алгоритм ассиметричной (двухключевой) системы шифрования данных RSA. Алгоритмы хэширования MD5, SHA. Федеральный закон Российской Федерации «Об электронной подписи» 6.04.2011г. № 63-ФЗ РФ Нормативно-правовые акты Российской Федерации о ведении электронного документооборота. Анализ моделей нарушителя; угрозы информационно-программному обеспечению вычислительных систем и их классификация.	СРС	10	ОПК-9	Л1.1 Л1.2 Л1.3
	Курсовая работа	СРС	36	ОПК-9	Л1.1 Л1.2 Л1.3
Экзамен – 36 часов					

Итого – 144 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	Фаронов А.Е.	Основы информационной безопасности при работе на компьютере	М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2020.— 154 с	Э1
Л1.2	Галатенко, В. А.	Основы информационной безопасности :	Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 с.	Э2
Л1.3	Шаньгин В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2019. — 702 с. — ISBN 978-5-4488-0070-2	Э3
5.1.2. Дополнительная литература				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**
Л2.1	М. М. Вулф, Н. Т. Разумовский, Р. Г. Прокди. .	Как защитить компьютер от вирусов	Спб: Наука и Техника, 2010. — 192 с.	Э4
5.1.3. Учебно-методическое обеспечение для самостоятельной работы обучающихся				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**
Л3.1	Гошко, С. В.	Технологии борьбы с компьютерными вирусами : практическое пособие	Москва : СОЛОН-ПРЕСС, 2016. — 351 с.	Э5

5.2. Электронные образовательные ресурсы	
Э1	https://www.iprbookshop.ru/89453.html
Э2	https://www.iprbookshop.ru/97562.html
Э3	https://www.iprbookshop.ru/87995.html
Э4	https://www.iprbookshop.ru/35399.html
Э5	https://www.iprbookshop.ru/90288.html

5.3. 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 посо-

бие / 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 экзамену осуществляется на протяжении всего времени изучения дисциплины.

Для более конкретной, целенаправленной и качественной подготовки к экзамену 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 кон-

трольные 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 экзамену, 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