ГОУ ВПО РОССИЙСКО-АРМЯНСКИЙ (СЛАВЯНСКИЙ) УНИВЕРСИТЕТ

Составлен в соответствии с государственными требованиями к минимуму содержания и уровню подготовки выпускников по направлению 11.03.03 КТЭС и Положением «ОбУМКД РАУ».

УТВЕРЖДАЮ:

Директор Института, к. ф.-м. наук Тирацуян А.А.

"19" июня 2023 г.

Институт: Математики и информатики

Кафедра: математической кибернетики

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС

Дисциплина: Б1.В.ДВ.03.02 «Информационные технологии»

Код и название дисциплины согласно учебному плану

Для бакалавриата:

Направление: 11.03.03 Конструирование и технология электронных средств

ЕРЕВАН

Структура и содержание УМКД

1. **Аннотация**

1.1. Системы компьютерной математики являются мощным и удобным инструментом в системе образования. Применение систем компьютерной математики позволяет производить трудоемкие численные расчеты, решать уравнения, упрощать сложные формулы, строить двумерные и трехмерные графики.Рассмотрение общих методов сбора, передачи, обработки и накопления информации, устройства компьютера, методов разработки алгоритмов решения задач, способов записи и реализации алгоритмов на языке высокого уровня

1.3. Для прохождения дисциплины студент должен

- ***знать***основы информатики и вычислительной техники, основы теории чисел;
- ***уметь*** применять отмеченные знания при решении соответствующих задач.

1.4. Дисциплины, изучение которых является необходимой базой для освоения данной дисциплины следующие - физика, математика, информатика, теория вероятностей и математическая статистика.

2. **Содержание**

2.1. ***Цель дисциплины*** – ознакомление студентов с основными понятиями и определениями теории информации и основ информационной безопасности, необходимыми для профессиональной деятельности в области информацинных технологий и телекоммуникаций. Изучение математического аппарата в области теории информации и различных методов криптографического закрытия информации, грамотного выбора паролей и способов постановки цифровой подписи.

Задача - ознакомление студентов с основными понятиями теории информации, проблемой обеспечения безопасности информационных систем, изучение различных угроз и методов защиты от них.

2.2. После изучения дисциплины студент должен:

- ***знать*** информационные характеристики источников сообщений и каналов передачи информации, методы и средства построения систем информационной безопасности;
- ***уметь*** использовать различные средства, принципы и методы кодирования, сжатия и шифрования информации для грамотного построения телекоммуникационных систем;
- ***иметь*** представление о свойствах информации и способов ее представления, об оценках предельного сжатия информации, о современных внешних и внутренних угрозах безопасности информационных систем и методах защиты от них;
- ***владеть*** методами синтеза и анализа криптографических систем и криптографических протоколов, закономерностями построения сложных криптографических схем.

2.3. Трудоемкость дисциплины: в академических часах – 108, в кредитах -3

2.3.1. Объем дисциплины и виды учебной работы

Виды учебной работы	Всего, в акад. часах
1. **Общая трудоемкость изучения дисциплины по семестрам, в т. ч.:**	**72**
1.1. Аудиторные занятия, в т. ч.:	**52**
1.1.1. Лекции	**18**
1.1.2. Практические занятия, в т. ч.	**-**
1.1.2.1. Обсуждение прикладных проектов	**-**
1.1.2.2. Кейсы	**-**
1.1.2.3. Деловые игры, тренинги	**-**
1.1.2.4. Контрольные работы	
1.1.2.5. Решение задач	**34**
1.1.3. Семинары	
1.1.4. Лабораторные работы	**-**
1.1.5. Другие виды (указать)	**-**
1.2. Самостоятельная работа, в т. ч.:	**20**
1.2.1. Подготовка к экзаменам	
1.2.2. Другие виды самостоятельной работы, в т.ч. (указать)	
1.2.2.1. Письменные домашние задания	
1.2.2.2. Курсовые работы	
1.2.2.3. Эссе и рефераты	
1.2.2.4. Другое (указать)	
1.3. Консультации	
1.4. Другие методы и формы занятий	
Итоговый контроль (экзамен, зачет, диф. зачет - указать)	**зачет**

2.3.2. Распределение объема дисциплины по темам и видам учебной работы

Разделы и темы дисциплины	**Всего (ак. часов)**	**Лекционные занятия (ак. часов)**	**Семинарские занятия (ак. часов)**	**Практические занятия (ак. часов)**	**Лабораторные работы (ак. часов)**
1	**2**	**3**	**4**	**5**	**6**
МОДУЛЬ 1.БАЗОВЫЕ ПОНЯТИЯ ИНФОРМАЦИОННОЙ ТЕХНОЛОГИИ	**10**	**4**		**6**	
Раздел 1. Информация, ее виды и формы представления	**6**	**1**		**6**	

Тема 1.1. Виды информации и способы ее представления в информационных системах	**3**	**1**		**2**	
Тема 1.2. Фазы обращения информации	**3**	**1**		**2**	
Тема 1.3. Способы измерения информации	**3**	**1**		**2**	
МОДУЛЬ 2. ОПРЕДЕЛЕНИЕ КОЛИЧЕСТВА ИНФОРМАЦИИ	**10**	**4**		**6**	
Раздел 2. Энтропия, как мера степени неопределенности	**5**	**2**		**3**	
Тема 2.1. Определение и свойства энтропии	**2**	**1**		**1**	
Тема 2.2.Энтропия непрерывного источника иформации	**3**	**1**		**2**	
Раздел 3.Измерение информации	**5**	**2**		**3**	
Тема 3.1.Определение и свойства информации	**4**	**1**		**2**	
Тема 3.2. Передача информации от дискретного источника	**2**	**1**		**1**	
МОДУЛЬ 3. ПРИЛОЖЕНИЕ ТЕОРИИ ИНФОРМАЦИИ К ЗАДАЧАМ ПЕРЕДАЧИ СООБЩЕНИЙ	**12**	**4**		**8**	
Раздел 4.Эффективное кодирование для канала без помех	**8**	**2**		**6**	
Тема 4.1. Информационная избыточность сообщений	**3**	**1**		**2**	
Тема 4.2. Алфавитное неравномерное двоичное кодирование	**5**	**1**		**4**	
Раздел 5.Передача сообщений при наличии помех	**4**	**2**		**2**	
Тема 5.1. Пропускная способность канала связи при наличии помех	**4**	**2**		**2**	

МОДУЛЬ 5. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ	**22**	**6**		**14**	
Раздел 8. Криптографическое закрытие информации	**12**	**4**		**10**	
Тема 8.1. Предмет и задачи криптографии и криптоанализа	**1**	**1**		**2**	
Тема 8.2. Классические шифры	**3**	**1**		**2**	
Тема 8.3. Симметричные криптосистемы	**4**	**1**		**3**	
Тема 8.4. Асимметричные криптосистемы	**4**	**1**		**3**	

Раздел 12. Специальные средства защиты.	**4**	**2**		**4**	
Тема 12.1. Защита помещений от подслушивания	**3**	**1**		**2**	
Тема 12.2. Средства выявления каналов утечки информации	**1**	**1**		**2**	
ИТОГО:	**54**	**18**		**34**	

2.3.3 Содержание разделов и тем дисциплины

МОДУЛЬ 1. БАЗОВЫЕ ПОНЯТИЯ ТЕОРИИ ИНФОРМАЦИИ

Введение

Краткая историческая справка о развитии теории информации. Постановка проблемы информационной безопасности. Основные понятия теории вероятностей. Некоторые законы распределения случайных величин. Содержание дисциплины [1,4].

Раздел 1. Информация, ее виды и формы представления

Тема 1.1. Виды информации и способы ее представления в информационных системах

Подходы к определению понятия «информация». Классификация информации по способу восприятия и форме представления. Сигнал, канал связи, сообщение, данные. Источник информации, приемник информации [1, Гл.1].

Тема 1.2. Фазы обращения информации

Принципы хранения, измерения, обработки и передачи информации. Меры количества и качества информации [1, Гл.1].

Тема 1.3. Способы измерения информации

Измерение количества информации, единицы измерения информации. Передача информации, скорость передачи информации [1, Гл.1].

МОДУЛЬ 2. ОПРЕДЕЛЕНИЕ КОЛИЧЕСТВА ИНФОРМАЦИИ

Раздел 2. Энтропия, как мера степени неопределенности

Тема 2.1. Определение и свойства энтропии

Дискретный источник информации, мера неопределенности выбора состояния источника. Свойства энтропии. Энтропия сложной системы. Условная энтропия [1, Гл.6; 2, Гл.1].

Тема 2.2. Энтропия непрерывного источника иформации

Относительная дифференциальная энтропия непрерывного источника информации. Условная энтропия, относительная дифференциальная условная энтропия непрерывного источника [3, Гл.8]

Раздел 3.Измерение информации

Тема 3.1. Определение и свойства информации

Общие понятия. Количество информации по Хартли и Шеннону. Объем информации. Взаимная информация [1, Гл. 6; 3, Гл. 4]

Тема 3.2. Передача информации от дискретного источника

Марковские и эргодические источники. Каналы связи. Количество информации, передаваемой по дискретному каналу [1, Гл.7]

МОДУЛЬ 3. ПРИЛОЖЕНИЕ ТЕОРИИ ИНФОРМАЦИИ К ЗАДАЧАМ ПЕРЕДАЧИ СООБЩЕНИЙ

Раздел 4.Эффективное кодирование для канала без помех

Тема 4.1. Информационная избыточность сообщений

Процесс передачи сообщения от источника к приемнику при отсутствии помех. Идеальный канал связи. Первичный алфавит, вторичный алфавит. Кодирование, декодирование. Информационная избыточность, полная информационная избыточность. Теорема Шеннона об источниках [3, Гл. 3; 1, Гл.7].

Тема 4.3. Алфавитное неравномерное двоичное кодирование

Принципы неравномерного кодирования. Основы префиксного кода. Неравенство Крафта. Префиксный код Шеннона-Фано, префиксный код Хаффмана [2, Гл. 2].

Раздел 5.Передача сообщений при наличии помех

Тема 5.1. Пропускная способность канала связи при наличии помех

Математическое описание линии связи с помехами. Пропускная способность канала с помехами [3, Гл.8].

МОДУЛЬ 4. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Раздел 6. Проблемы и задачи информационной безопасности

Тема 6.1. Основные понятия и составляющие информационной безопасности

Современное состояние, перспектива и ретроспектива. Информационные системы, средства, каналы, сети и среды. Основные понятия, определения и составляющие информационной безопасности. Наиболее опасные угрозы информационной безопасности. Информационные атаки. Технические каналы утечки информации. Основные задачи защиты информации [4, Гл.1].

Тема 6.2. Политика информационной безопасности

Уровни формирования режима информационной безопасности. Стандарты информационной безопасности. Административный уровень обеспечения информационной безопасности. Анализ и оценка рисков информационной безопасности [4, Гл.6, Гл.7].

Тема 6.3. Механизмы обеспечения информационной безопасности

Идентификация и аутентификация. Биометрическая аутентификация. Разграничение доступа. Регистрация и аудит. Технология виртуальных частных сетей. [4, Гл.10; Гл.17].

Раздел 7. Информационная безопасность компьютерных сетей

Тема 7.1. Вредоносные программы и защита от них

Классификация вредоносного программного обеспечения. Антивирусные программы [4, Гл.13].

Тема 7.2. Особенности обеспечения информационной безопасности в компьютерных сетях

Локальные и сетевые (удаленные) угрозы. Сетевые модели передачи данных. Модель взаимодействия открытых систем OSI/ISO. Стек протоколов TCP/IP. Классификация удаленных угроз в вычислительных сетях [4, Гл.15].

МОДУЛЬ 5. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Раздел 8. Криптографическое закрытие информации

Тема 8.1. Предмет и задачи криптографии и криптоанализа

Предмет и задачи криптографии и криптоанализа. История развития криптографии.Стойкость криптографического алгоритма. Классификация криптографических алгоритмов [5, Гл.1].

Тема 8.2. Классические шифры

Классические шифры перестановки: шифр «скитала», решетка Кардано. Шифры простой замены: квадрат Полибия, шифрующая система Цезаря. Криптоанализ шифров простой замены. Шифр Вижинера. Шифр Вернама. Шифры колонной замены. Шифровальные машины [5, Гл.1].

Тема 8.3. Симметричные криптосистемы

Основы теории Шенонна и ее развитие. Модели шифров. Результаты теории информации для криптографии. Композиции шифров. Сеть Фейстеля. Алгоритм шифрования DES, основные режимы работы. Шифр AES. Вычислительная стойкость криптоалгоритмов. Атаки на алгоритмы шифрования. Методы криптоанализа блочных шифров. Требования, предъявляемые к современным блочным алгоритмам шифрования. Генерация, распределение и хранение ключей шифрования для симметричных систем. Генераторы случайных и псевдослучайных чисел [5, Гл.2].

Тема 8.4. Асимметричные криптосистемы

Ассиметричные системы шифрования, их особенности, преимущества и недостатки. Сравнение с симметричными системами. Система Диффи-Хеллмана. Математические основы асимметричной криптографии. Шифр Шамира. Шифр Эль-Гамаля. Шифр RSA. Атаки на алгоритм RSA [5, Гл.3].

Раздел 9. Контроль целостности данных

Тема 9.1. Электронная цифровая подпись

Целостность данных. Функции хэширования. Требования к хэш-функциям. Общие положения электронной цифровой подписи. Примеры электронной цифровой подписи на основе алгоритмов с открытыми ключами [5, Гл.3].

Тема 9.2. Современные приложения криптографии

Системы тайного электронного голосования. Электронные деньги. Электронная жеребьевка. Защита документов и ценных бумаг от подделки. Стеганографические методы защиты информации [5, Гл.3].

МОДУЛЬ 6. БАЗОВЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ ДАННЫХ В СИСТЕМАХ МОБИЛЬНОЙ СВЯЗИ И ЭЛЕКТРОННОЙ ИДЕНТИФИКАЦИИ

Раздел 10. Аспекты безопасности в сотовых системах подвижной радиосвязи

Тема 10.1. Техническая безопасность в стандартах подвижной связи GSM и CDMA

Угрозы сообщению. Угрозы пользователю. Угрозы системе. Протоколы шифрования/дешифрования в стандартах подвижной связи GSM и CDMA [6, Гл.11, Гл.13]

Тема 10.2. Техническая безопасность в стандарте подвижной связи LTE

Алгоритмы шифрования, идентификации и аутентификации в стандарте LTE [6, Гл.13]

Раздел 11. Обеспечение информационной безопасности систем электронной идентификации

Тема 11.1. Обеспечение безопасности данных в системах RFID

Обеспечение целостности и конфиденциальности передаваемых данных. Взаимная аутентификация ридера и транспондера [7, Гл.12].

Раздел 12. Специальные средства защиты

Тема 12.1.Защита помещений от подслушивания

Звукопоглощающие материалы и конструкции. Звукоизоляция помещений. Помехоподавляющие фильтры. [14, Гл.1].

Тема 12.2. Средства выявления каналов утечки информации

Индикаторы электромагнитного поля. Сканирующие радиоприемники. Анализаторы спектра, радиочастотомеры. Многофункциональные комплексы для выявления каналов утечки информации [14, Гл.3].

2.3.4. Краткое содержание практических занятий - 36 часов.

1. Способы хранения, обработки и передачи информации
2. Единицы измерения информации
3. Носители информации
4. Определение объема данных в двоичной и десятичной системах счисления
5. Оценка условной энтропии ансамбля сообщений
6. Физическая сущность условной энтропии
7. Энтропия сложной системы
8. Поиск энтропии случайных величин.
9. Определение количества информации в равновероятном и не равновероятном сообщении
10. Взаимная информация
11. Определение скорости передачи информации
12. Скорость передачи информации при испольвании кода Бодо
13. Основы кодирования сообщений: первичный и вторичный алфавиты, оптимальный код
14. Общая и частная избыточности алфавита
15. Избыточность сообщений при побуквенном и блочном кодировании

16. Алфавитное кодирование с неравной длительностью сигналов
17. Принципы нерваномерного кодирования
18. Основы префиксного кода
19. Установление связи средней длины кода с энтропией
20. Кодирование по методу Шеннона-Фано
21. Кодирование по методу Хаффмана
22. Сжатие данных
23. Установление связи ширины полосы канала со скоростью передачи информации
24. Программно-аппаратные средства обеспечения информационной безопасности в компьютерных сетях
25. Защита программного обеспечения от вирусного заражения, разрушающих программных действий и изменений
26. Особенности защиты информации в компьютерных сетях
27. Уровни сетевых атак согласно модели OSI
28. Виды атак на сетевые компоненты. Атаки на DNS- сервера
29. Использование классических криптоалгоритмов перестановки и подстановки для защиты текстовой информации
30. Изучение устройства и принципа работы шифровальной машины «Энигма»
31. Шифры гаммирования
32. Результаты теории информации для криптографии, теорема Шеннона
33. Дешифрование шифра простой перестановки при помощи метода биграмм
34. Сеть Фейстеля
35. Стандарт симметричного шифрования DES
36. Генерация псевдослучайных чисел методом Блюм-Блюма-Шуба
37. Понятие односторонней функции. Использование односторонних функций в криптографических алгоритмах
38. Теория сложности и криптография
39. Система Диффи-Хеллмана
40. Математические основы асимметричной криптографии: фунцкия Эйлера, малая теорема Ферма, теорема Эйлера, расширенный алгоритм Евклида,алогоритм повторного умножения по модулю, алгоритм повторного возведения в квадрат по модулю
41. Проверка чисел на простоту, тест Миллера-Рабина
42. Шифр Шамира
43. Шифр Эль-Гамаля
44. Алгоритм RSA
45. Безопасность алгоритма RSA и виды основных атак
46. Электронная цифровая подпись на основе RSA
47. Электронная цифровая подпись на основе схемы Эль-Гамаля
48. Создание скрытого канала передачи информации
49. Скрытие речевой информации в телефонных системах с использованием криптографических методов
50. Применение криптографических алгоритмов A3, A8 и A5
51. Взаимная аутентификация с использованием секретного криптоключа
52. Взаимная аутентификация с использованием выведенных криптоключей

2.4. Материально-техническое обеспечение дисциплины

- Учебные методические пособия
- Вычислительная техника

- Проектор
- Слайдоскоп

2.5. Распределение весов по модулям и формам контроля

Формы контролей	**Веса форм текущих контролей в результирующих оценках текущих контролей**			**Веса форм промежуточных контролей в оценках промежуточных контролей**			**Веса оценок промежуточных контролей и результирующих оценок текущих контролей в итоговых оценках промежуточных контролей**			**Веса итоговых оценок промежуточных контролей в результирующей оценке промежуточных контролей**	**Веса результирующей оценки промежуточных контролей и оценки итогового контроля в результирующей оценке итогового контроля**
Вид учебной работы/контроля	**М1[1]**	**М2**	**М3**	**М1**	**М2**	**М3**	**М1**	**М2**	**М3**		
Контрольная работа											
Тест											
Курсовая работа											
Лабораторные работы		1	1								
Письменные домашние задания											
Реферат											
Эссе											
Семинары											
Решение задач											
Веса результирующих оценок текущих контролей в итоговых оценках промежуточных контролей								1	1		
Веса оценок промежуточных контролей в итоговых оценках промежуточных контролей											
Вес итоговой оценки 1-го промежуточного контроля в результирующей оценке промежуточных контролей										-	
Вес итоговой оценки 2-го промежуточного контроля в результирующей оценке промежуточных контролей										0.5	
Вес итоговой оценки 3-го промежуточного контроля в результирующей оценке промежуточных контролей										0.5	
Вес результирующей оценки											0.4

[1] Учебный Модуль

промежуточных контролей в результирующей оценке итогового контроля											
Экзамен/зачет (оценка итогового контроля)											(Зачет) 0.6
	Σ = 1	**Σ = 1**	**Σ = 1**	**Σ = 1**	**Σ = 1**	**Σ = 1**	**Σ = 1**	**Σ = 1**	**Σ = 1**	**Σ = 1**	**Σ = 1**

3. **Теоретический блок**

Рекомендуемая литература

а) Базовые учебники

1. **Костров Б. В.** Основы цифровой передачи и кодирования информации.-М.: «ТехБук», 2007.-192 с.
2. **Кудряшов Б. Д.** Теория информации: Учебник для вузов.-СПб.:Питер, 2009.- 320 с.
3. **Вернер М.** Основы кодирования: Учебник для ВУЗов.-М.: Техносфера, 2004.- 288с.
4. **Макаренко С. И.** Информационная безопасность: учебное пособие для студентов вузов. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с.: ил.
5. **Васильева И. Н.** Криптографические методы защиты информации: учебник и практикум для академического бакалавриата.-М.: Издательство Юрайт, 2017.-349 с.

б) Дополнительная литература:

6. **Бабков В. Ю., Цикин И. А.** Сотовые системы мобильной радиосвязи: учеб. пособие.-2-е изд., перераб. и доп.-СПб.:БХВ-Петербург, 2013.- 432 с.
7. **Дшхунян В. Л., Шаньгин В. Ф.** Электронная идентификация. Бесконтактные идентификаторы и смарт-карты.- М.: «Издательство АСТ»: Издательство «НТ Пресс», 2004.-695 с.
8. **Блинова И. В., Попов И. Ю.** Теория информации. Учебное пособие. – СПб.: Университет ИТМО, 2018. – 84 с.
9. **Галатенко В. А.** Основы информационной безопасности. – М: Интернет-Университет Информационных Технологий – ИНТУИТ.РУ, 2003.
10. **Баранова Е. К.** Криптографические методы защиты информации. Лабораторный практикум: учебное пособие / Е.К. Баранова, А.В.Бабаш .- М.: КНОРУС, 2015.- 200 с.
11. **Рид Р.** Основы теории передачи информации: пер. с англ./ Р.Рид; Пер. М.В. Бойко; Под ред. Е.В. Гусевой.-М.: Вильямс, 2005.-293 с.
12. **ТаирянВ. И.** Основы информационной безопасности в компьютерных сетях. Учебное пособие, Изд-во РАУ, 2006.

13. **Белов В. М., Новиков С. Н., Солонская О. И.** Теория информации. Курс лекций. Учебное пособие для вузов.-М.: Горячая линия-Телеком, 2012.-143 с.

14. **Технические средства и методы защиты информации: Учебник для вузов** / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО «Издательство Машиностроение», 2009 – 508 с.

4. Перечень вопросов итогового контроля

1. Подходы к определению понятия «информация»
2. Классификация информации по способу восприятия и форме представления.
3. Сигнал, канал связи, сообщение, данные. Источник информации, приемник информации
4. Принципы хранения, измерения, обработки и передачи информации
5. Меры количества и качества информации
6. Измерение количества информации, единицы измерения информации
7. Передача информации, скорость передачи информации
8. Дискретный источник информации, мера неопределенности выбора состояния источника.
9. Свойства энтропии, энтропия сложной системы, условная энтропия
10. Относительная дифференциальная энтропия непрерывного источника информации
11. Условная энтропия, относительная дифференциальная условная энтропия непрерывного источника
12. Количество информации по Хартли и Шеннону, объем информации, взаимная информация
13. Марковские и эргодические источники. Каналы связи
14. Количество информации, передаваемой по дискретному каналу
15. Процесс передачи сообщения от источника к приемнику при отсутствии помех
16. Идеальный канал связи. Первичный алфавит, вторичный алфавит. Кодирование, декодирование
17. Информационная избыточность
18. Неравенство Крафта
19. Теорема Шеннона об источниках
20. Принципы неравномерного кодирования.

21. Основы префиксного кода. Префиксный код Шеннона-Фано, префиксный код Хаффмана

22. Математическое описание линии связи с помехами. Пропускная способность канала с помехами

23. Основные понятия, определения и составляющие информационной безопасности

24. Наиболее опасные угрозы информационной безопасности

25. Информационные атаки. Технические каналы утечки информации

26. Уровни формирования режима информационной безопасности.

27. Стандарты информационной безопасности.

28. Административный уровень обеспечения информационной безопасности

29. Анализ и оценка рисков информационной безопасности

30. Идентификация и аутентификация. Биометрическая аутентификация

31. Разграничение доступа. Регистрация и аудит

32. Технология виртуальных частных сетей

33. Классификация вредоносного программного обеспечения. Антивирусные программы

34. Сетевые модели передачи данных. Модель взаимодействия открытых систем OSI/ISO. Стек протоколов TCP/IP

35. Классификация удаленных угроз в вычислительных сетях

36. Предмет и задачи криптографии и криптоанализа. Стойкость криптографического алгоритма. Классификация криптографических алгоритмов

37. Классические шифры перестановки: шифр «скитала», решетка Кардано. Шифры простой замены: квадрат Полибия, шифрующая система Цезаря. Криптоанализ шифров простой замены

38. Шифр Вижинера. Шифр Вернама. Шифры колонной замены. Шифровальные машины

39. Основы теории Шенонна и ее развитие. Модели шифров. Результаты теории информации для криптографии

40. Композиции шифров. Сеть Фейстеля

41. Алгоритм шифрования DES, основные режимы работы

42. Шифр AES

43. Вычислительная стойкость криптоалгоритмов. Атаки на алгоритмы шифрования

44. Методы криптоанализа блочных шифров. Требования, предъявляемые к современным блочным алгоритмам шифрования

45. Генерация, распределение и хранение ключей шифрования для симметричных систем, генераторы случайных и псевдослучайных чисел

46. Ассиметричные системы шифрования, их особенности, преимущества и недостатки. Сравнение с симметричными системами

47. Система Диффи-Хеллмана

48. Математические основы асимметричной криптографии.

49. Шифр Шамира. Шифр Эль-Гамаля

50. Шифр RSA. Атаки на алгоритм RSA

51. Целостность данных. Функции хэширования. Требования к хэш-функциям

52. Общие положения электронной цифровой подписи. Примеры электронной цифровой подписи на основе алгоритмов с открытыми ключами

53. Системы тайного электронного голосования. Электронные деньги. Электронная жеребьевка. Защита документов и ценных бумаг от подделки. Стеганографические методы защиты информации

54. Угрозы сообщению. Угрозы пользователю. Угрозы системе

55. Протоколы шифрования/дешифрования в стандартах подвижной связи GSM и CDMA

56. Алгоритмы шифрования, идентификации и аутентификации в стандарте LTE

57. Обеспечение целостности и конфиденциальности передаваемых данных. Взаимная аутентификация ридера и транспондера

58. Защита помещений от подслушивания.

59. Средства выявления каналов утечки информации

Учебная программа:

одобрена Кафедрой телекоммуникации

Зав. кафедрой: А.К. Агаронян _____

(подпись)