ГОУ ВПО РОССИЙСКО-АРМЯНСКИЙ (СЛАВЯНСКИЙ) УНИВЕРСИТЕТ

Составлен в соответствии с государственными требованиями к минимуму содержания и уровню подготовки выпускников по направлению 11.03.02 Инфокоммуникационные технологии и системы связи и Положением «Об УМКД РАУ».

УТВЕРЖДАЮ:

Директор института

А.А. Саркисян

«21» июля 2023

Утвержден Ученым Советом ИФИ протокол № 33

Инженерно-физический институт

Кафедра Телекоммуникаций

Автор(ы): *кандидат тех. наук, доцент Бадалян Б.Ф.*

Ученое звание, ученая степень, Ф.И.О

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС

Дисциплина: Б1.В.07 «Криптография и безопасность»

Код и название дисциплины согласно учебному плану

Для магистратуры:

Направление: 11.04.02 Инфокоммуникационные технологии и системы связи

Магистерская программа: 071301.00.7 «Беспроводные коммуникации и сенсоры»

ЕРЕВАН

Структура и содержание УМКД

1. Аннотация

1.1. В курсе дисциплины “Криптография и безопасность” излагаются основные понятия криптографических методов и средств защиты информации, необходимые для профессиональной деятельности в области информационных технологий и систем связи. Рассматриваются общие характеристики методов криптографической защиты информации, приводятся описание средств, принципов и механизмов обеспечения информационной безопасности и средств защиты компьютерной информации с применением криптографии. Даны определения и примеры криптографического закрытия информации. Подробно рассмотрены классические и современные симметричные и асимметричные криптосистемы шифрования, методы создания цифровой подписи, специальные технические средства для защиты помещений и аппаратуры. Описываются процедуры аутентификации и шифрования в системах радиочастотной идентификации и мобильной радиосвязи разных поколений.

1.2. Данная дисциплина теснейшим образом связана со следующими дисциплинами: математика, информатика, теория кодирования, общая теория связи, построение телекоммуникационных сетей и систем.

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 криптографии и информационной безопасности, необходимыми для профессиональной деятельности в области информационных технологий и телекоммуникаций. Изучение математического аппарата в области различных методов криптографического закрытия информации, грамотного выбора паролей и способов постановки цифровой подписи.

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

2.2. После изучения дисциплины студент должен:

- ***знать*** основные меры и фазы обращения информации в различных информационных системах, методы и средства построения систем информационной безопасности;

- ***уметь*** использовать различные средства, принципы и шифрования/расшифровки информации для грамотного построения телекоммуникационных систем;

- ***иметь*** представление о свойствах информации и способов ее представления, 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, а также механизмами защиты информационных систем от вредоносных программ.

2.3. Трудоемкость дисциплины: в академических часах – 72, в кредитах -2

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.:	**34**
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	**16**
1.1.3. Семинары	
1.1.4. Лабораторные работы	**-**
1.1.5. Другие виды (указать)	**-**
1.2. Самостоятельная работа, в т. ч.:	**38**
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 ТЕОРИИ ИНФОРМАЦИИ	**5**	**3**		**2**	
Введение	**1**	**1**			
Раздел 1. Информация, ее виды и формы представления	**3**	**2**		**1**	
Тема 1.1. Виды информации и способы ее представления в информационных системах	**1**	**1**			

Тема 1.2. Фазы обращения и способы измерения информации	**2**	**1**		**1**	

МОДУЛЬ 2. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ	**8**	**6**		**3**	
Раздел 2. Проблемы и задачи информационной безопасности	**3**	**3**			
Тема 2.1. Основные понятия и составляющие информационной безопасности	**1**	**1**			
Тема 2.2. Политика информационной безопасности	**1**	**1**			
Тема 2.3. Механизмы обеспечения информационной безопасности	**1**	**1**	**-**	**-**	
Раздел 3. Информационная безопасность компьютерных сетей	**5**	**2**		**3**	
Тема 3.1. Вредоносные программы и защита от них	**3**	**1**	**-**	**2**	
Тема 3.2. Особенности обеспечения информационной безопасности в компьютерных сетях	**2**	**1**		**1**	

МОДУЛЬ 3. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ	**18**	**7**		**11**	
Раздел 4. Криптографическое закрытие информации	**13**	**4**		**9**	
Тема 4.1. Предмет и задачи криптографии и криптоанализа	**1**	**1**			
Тема 4.2. Классические шифры	**3**	**1**		**2**	
Тема 4.3. Симметричные криптосистемы	**5**	**1**		**4**	
Тема 4.4. Асимметричные криптосистемы	**4**	**1**		**3**	
Раздел 5. Контроль целостности данных	**5**	**3**		**2**	
Тема 5.1. Электронная цифровая подпись	**4**	**2**		**2**	
Тема 5.2. Современные приложения криптографии	**1**	**1**		**-**	
МОДУЛЬ 4. БАЗОВЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ ДАННЫХ В СИСТЕМАХ МОБИЛЬНОЙ СВЯЗИ И ЭЛЕКТРОННОЙ ИДЕНТИФИКАЦИИ	**4**	**2**		**2**	
Раздел 6. Аспекты безопасности в сотовых системах подвижной радиосвязи	**2**	**1**	**-**	**1**	
Тема 6.1. Техническая безопасность в стандартах подвижной связи GSM, CDMA и LTE	**2**	**1**	**-**	**1**	
Раздел 7. Обеспечение информационной безопасности систем электронной идентификации	**2**	**1**	**-**	**1**	
Тема 7.1. Обеспечение безопасности данных в микропроцессорных картах и системах RFID	**2**	**1**		**1**	
ИТОГО:	**36**	**18**		**18**	

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 [1,2].

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 и способы измерения информации

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

МОДУЛЬ 2. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Раздел 2. Проблемы и задачи информационной безопасности

Тема 2.1. 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 [2, Гл.1].

Тема 2.2. Политика информационной безопасности

Уровни формирования режима информационной безопасности. Стандарты информационной безопасности. Административный уровень обеспечения информационной безопасности. Анализ и оценка рисков информационной безопасности [2, Гл.6, Гл.7].

Тема 2.3. Механизмы обеспечения информационной безопасности

Идентификация и аутентификация. Биометрическая аутентификация. Разграничение доступа. Регистрация и аудит. Технология виртуальных частных сетей. [2, Гл.10; Гл.17].

Раздел 3. Информационная безопасность компьютерных сетей

Тема 3.1. Вредоносные программы и защита от них

Классификация вредоносного программного обеспечения. Антивирусные программы [2, Гл.13].

Тема 3.2. 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 [2, Гл.15].

МОДУЛЬ 3. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Раздел 4. Криптографическое закрытие информации

Тема 4.1. Предмет и задачи криптографии и криптоанализа

Предмет и задачи криптографии и криптоанализа. История развития криптографии.Стойкость криптографического алгоритма. Классификация криптографических алгоритмов [3, Гл.1].

Тема 4.2. 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 [3, Гл.1].

Тема 4.3. 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 [3, Гл.2].

Тема 4.4. 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 [3, Гл.3].

Раздел 5. Контроль целостности данных

Тема 5.1. 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 [3, Гл.3].

Тема 5.2. Современные приложения криптографии

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

МОДУЛЬ 4. БАЗОВЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ ДАННЫХ В СИСТЕМАХ МОБИЛЬНОЙ СВЯЗИ И ЭЛЕКТРОННОЙ ИДЕНТИФИКАЦИИ

Раздел 6. Аспекты безопасности в сотовых системах подвижной радиосвязи

Тема 6.1. Техническая безопасность в стандартах подвижной связи GSM, CDMA и LTE

Угрозы сообщению. Угрозы пользователю. Угрозы системе. Протоколы шифрования/дешифрования в стандартах подвижной связи GSM, CDMA и LTE [4, Гл.11, Гл.13]

Раздел 7. Обеспечение информационной безопасности систем электронной идентификации

Тема 7.1. Обеспечение безопасности данных в микропроцессорных картах и системах RFID

Обеспечение целостности и конфиденциальности передаваемых данных. Взаимная аутентификация ридера и транспондера [5, Гл.12].

2.3.4. Краткое содержание практических занятий - 18 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. Определение скорости передачи информации
6. Скорость передачи информации при испольвании кода Бодо
7. Программно-аппаратные средства обеспечения информационной безопасности в компьютерных сетях
8. Защита программного обеспечения от вирусного заражения, разрушающих программных действий и изменений
9. Особенности защиты информации в компьютерных сетях
10. Уровни сетевых атак согласно модели OSI
11. Виды атак на сетевые компоненты. Атаки на DNS- сервера
12. Использование классических криптоалгоритмов перестановки и подстановки для защиты текстовой информации
13. Способы скрытой передачи данных
14. Сокрытие информации в звуковых файлах формата MIDI и WAV
15. Изучение устройства и принципа работы шифровальной машины «Энигма»
16. Шифры гаммирования
17. Результаты теории информации для криптографии, теорема Шеннона
18. Дешифрование шифра простой перестановки при помощи метода биграмм

19. Сеть Фейстеля
20. Стандарт симметричного шифрования DES
21. Генерация псевдослучайных чисел методом Блюм-Блюма-Шуба
22. Понятие односторонней функции. Использование односторонних функций в криптографических алгоритмах
23. Теория сложности и криптография
24. Система Диффи-Хеллмана
25. 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
26. Проверка чисел на простоту, тест Миллера-Рабина
27. Шифр Шамира
28. Шифр Эль-Гамаля
29. Алгоритм RSA
30. Безопасность алгоритма RSA и виды основных атак
31. Электронная цифровая подпись на основе RSA
32. Электронная цифровая подпись на основе схемы Эль-Гамаля
33. Создание скрытого канала передачи информации
34. Скрытие речевой информации в телефонных системах с использованием криптографических методов
35. Применение криптографических алгоритмов A3, A8 и A5
36. Взаимная аутентификация с использованием секретного криптоключа
37. 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					1						
Тест											
Курсовая работа											
Лабораторные работы											
Письменные домашние задания											
Реферат											
Эссе											
Семинары											
Решение задач	1										
Веса результирующих оценок текущих контролей в итоговых оценках промежуточных контролей								0.5			
Веса оценок промежуточных контролей в итоговых оценках промежуточных контролей								0.5			
Вес итоговой оценки 1-го промежуточного контроля в результирующей оценке промежуточных контролей											
Вес итоговой оценки 2-го промежуточного контроля в результирующей оценке промежуточных контролей										1	
Вес итоговой оценки 3-го промежуточного контроля в результирующей оценке промежуточных контролей											
Вес результирующей оценки промежуточных контролей в результирующей оценке итогового контроля											0.4
Экзамен/зачет (оценка итогового контроля)											(Зачет) 0.6
	∑ = 1	**∑ = 1**	**∑ = 1**	**∑ = 1**	**∑ = 1**	**∑ = 1**	**∑ = 1**	**∑ = 1**	**∑ = 1**	**∑ = 1**	**∑ = 1**

[1] Учебный Модуль

3. Теоретический блок

Рекомендуемая литература

а) Базовые учебники

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

б) **Дополнительная литература**:

4. **Бабков В. Ю., Цикин И. А.** Сотовые системы мобильной радиосвязи: учеб. пособие.-2-е изд., перераб. и доп.-СПб.:БХВ-Петербург, 2013.- 432 с.
5. **Дшхунян В. Л., Шаньгин В. Ф.** Электронная идентификация. Бесконтактные идентификаторы и смарт-карты.- М.: «Издательство АСТ»: Издательство «НТ Пресс», 2004.-695 с.
6. **Блинова И. В., Попов И. Ю.** Теория информации. Учебное пособие. – СПб.: Университет ИТМО, 2018. – 84 с.
7. **Карпухин Е.О.** Технологии и методы защиты инфокоммуникационных систем и сетей. Учебное пособие для вузов.-М.:Горячая линия-Телеком, 2020.-120 с.
8. **Баранова Е. К.** Криптографические методы защиты информации. Лабораторный практикум: учебное пособие / Е.К. Баранова, А.В.Бабаш .- М.: КНОРУС, 2015.- 200 с.
9. **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.
10. **Таирян В. И.** Основы информационной безопасности в компьютерных сетях. Учебное пособие, Изд-во РАУ, 2006.
11. **Телекоммуникационные системы и сети: Учебное пособие. В 3 томах. Том 1. – Современные технологии /** Б. И. Крук, В. Н. Попантонопуло, В. П. Шувалов; под ред. профессора В. П. Шувалова. – Изд. 4-е, испр**.** и доп. – М.: Горячая линия–Телеком, 2012. – 620 с.
12. **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. Основные понятия, определения и составляющие информационной безопасности
9. Наиболее опасные угрозы информационной безопасности
10. Информационные атаки. Технические каналы утечки информации
11. Уровни формирования режима информационной безопасности.
12. Стандарты информационной безопасности.
13. Административный уровень обеспечения информационной безопасности
14. Анализ и оценка рисков информационной безопасности
15. Идентификация и аутентификация. Биометрическая аутентификация
16. Разграничение доступа. Регистрация и аудит
17. Технология виртуальных частных сетей
18. Классификация вредоносного программного обеспечения. Антивирусные программы
19. Сетевые модели передачи данных. Модель взаимодействия открытых систем OSI/ISO. Стек протоколов TCP/IP
20. Классификация удаленных угроз в вычислительных сетях
21. Предмет и задачи криптографии и криптоанализа. Стойкость криптографического алгоритма. Классификация криптографических алгоритмов
22. Классические шифры перестановки: шифр «скитала», решетка Кардано. Шифры простой замены: квадрат Полибия, шифрующая система Цезаря. Криптоанализ шифров простой замены
23. Шифр Вижинера. Шифр Вернама. Шифры колонной замены. Шифровальные машины
24. Основы теории Шенонна и ее развитие. Модели шифров. Результаты теории информации для криптографии
25. Композиции шифров. Сеть Фейстеля
26. Алгоритм шифрования DES, основные режимы работы
27. Шифр AES

28. Вычислительная стойкость криптоалгоритмов. Атаки на алгоритмы шифрования
29. Методы криптоанализа блочных шифров. Требования, предъявляемые к современным блочным алгоритмам шифрования
30. Генерация, распределение и хранение ключей шифрования для симметричных систем, генераторы случайных и псевдослучайных чисел
31. Ассиметричные системы шифрования, их особенности, преимущества и недостатки. Сравнение с симметричными системами
32. Система Диффи-Хеллмана
33. Математические основы асимметричной криптографии.
34. Шифр Шамира. Шифр Эль-Гамаля
35. Шифр RSA. Атаки на алгоритм RSA
36. Целостность данных. Функции хэширования. Требования к хэш-функциям
37. Общие положения электронной цифровой подписи. Примеры электронной цифровой подписи на основе алгоритмов с открытыми ключами
38. Системы тайного электронного голосования. Электронные деньги. Электронная жеребьевка. Защита документов и ценных бумаг от подделки. Стеганографические методы защиты информации
39. Угрозы сообщению. Угрозы пользователю. Угрозы системе
40. Протоколы шифрования/дешифрования в стандартах подвижной связи GSM и CDMA
41. Алгоритмы шифрования, идентификации и аутентификации в стандарте LTE
42. Обеспечение целостности и конфиденциальности передаваемых данных. Взаимная аутентификация ридера и транспондера

Учебная программа:

одобрена Кафедрой телекоммуникации

Зав. кафедрой: А.К. Агаронян _____

(подпись)