# ГОУ ВПО РОССИЙСКО-АРМЯНСКИЙ УНИВЕРСИТЕТ

**Составлен в соответствии с государственными требованиями к минимуму содержания и уровню подготовки выпускников по направлению 01.04.02 Прикладная математика и информатика и Положением «Об УМКД РАУ».**

**УТВЕРЖДАЮ:**
**Директор института математики и информатики**
**к.ф.-м.н.,**
**Дарбинян Арман Араикович**
**"19" 07 2023г.**

**Институт Математики и информатики**

**Кафедра: Математической кибернетики**

*Автор(ы): к.ф.-м.н.,* **Абраамян Сергей Енокович**

## *УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС*

**Дисциплина Б1.В.ДВ.01.01: «Криптографическая защита информации»**

**Направление: «Прикладная математика и информатика»01.04.02**

**Основная образовательная программа магистратуры: 01.04.02 «Математическое и программное обеспечение защиты информации»**

**ЕРЕВАН**

## 1 Цели изучения дисциплины

Изучение Криптографическая защита информации является важнейшей частью подготовки по специальности «Прикладная математика и информатика». Это объясняется той ролью, которую данная теория играет в системах компьютерной безопасности любой организации.

Изучение криптографическая защита информации предполагает изучение вопросов, касающихся фундаментальных аспектов понятия "безопасность", а также знакомство с криптографическими алгоритмами, рядом особенностей присущих каждому из них.

Такой подход позволяет систематизировать знания о криптографии, придать им упорядоченный характер.

Учебная дисциплина «Теория кодирования» формирует теоретические знания и навыки при проектировании и реализации алгоритмов кодирования, применительно к определенной отрасли жизнедеятельности.

Целью изучения дисциплины «Криптографическая защита информации» является формирование прочной теоретической базы для понимания алгоритмов криптографии, а также их использования при работе с данными различного происхождения.

Задачами изучения дисциплины «Криптографическая защита информации» являются:

- знакомство студентов с основными понятиями криптографии;
- изучение использовать криптографические алгоритмы;

## 2. Требования к уровню освоения программы

Изучение данной дисциплины в комплексе с другими учебными дисциплинами формирует профессиональные знания информатиков. В результате изучения дисциплины студент должен:

**Иметь представление**:

- о роли и месте знаний по дисциплине «Криптографическая защита информации» при освоении смежных дисциплин по выбранной специальности и в сфере профессиональной деятельности;
- об основных понятиях теории информации и алгоритмах эффективного шифрования;

**Знать:**

- основы криптографии;
- алгоритмы эффективного криптографии.

**Уметь:**

- применять алгоритмы эффективного шифрования для конкретной задачи;
- самостоятельно обучаться использованию современных алгоритмов теории кодирования.

**Иметь навык:**
- составлять эффективные коды для кодирования данных различной природы.

**2.**

| **Виды учебной работы** | **Всего часов** | **Распределение по семестрам** | | | |
|---|---|---|---|---|---|
| | | **1 сем.** | **2 сем.** | **3 сем.** | **4 сем.** |
| **1** | **2** | **3** | | **5** | **6** |
| 1. Общая трудоемкость изучения дисциплины по семестрам, в т. ч.: | **72** | | | **72** | |
| 1.1. Аудиторные занятия, в т. ч.: | **36** | | | **36** | |
| 1.1.1. Лекции | **18** | | | **18** | |
| 1.1.2. Лдабораторные занятия | | | | | |
| 1.1.3. Практические занятия | **18** | | | **18** | |
| 3.Самостоятельная работа, в т. ч.: | **18** | | | **18** | |
| 3. Контроль | **18** | | | **18** | |
| 5. Кредиты | **2** | | | **2** | |
| 6.Форма итогового контроля: Экзамен/Зачет | **зач.** | | | **зач.** | |

| **Разделы и темы дисциплины** | **Всего (ак. часов)** | **Лекции(ак. часов)** | **Практ. занятия (ак. часов)** | **Семина-ры (ак. часов)** | **Лабор. (ак. часов)** | **Другие виды занятий (ак. часов)** |
|---|---|---|---|---|---|---|
| **1** | **2=3+4+5+6+7** | **3** | **4** | **5** | **6** | **7** |
| | | | | | | |
| | | | | | | |
| **Тема 1. Введение.** | **6** | **3** | **3** | | | |
| **Тема 2. Цифровой сертификат** | **6** | **3** | **3** | | | |
| **Тема 3. Защищенное или тайное многостороннее вычисление.** | **6** | **3** | **3** | | | |
| **Тема 4. Гомоморфное шифрование** | **6** | **3** | **3** | | | |
| **Тема 5. Шифрование с сохранением порядка** | **6** | **3** | **3** | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Тема 6. Proxy re-encryption.** | **6** | **3** | **3** | | | |
| **ИТОГО** | **36** | **18** | **18** | | | |

## 3 Содержание тем

**ТЕМА № 1. Введение.**
Криптография с открытым ключом, Алгоритмы цифровой подписи, Хэш функции
**ТЕМА № 2. Цифровой сертификат (Сертификат открытого ключа)**
**ТЕМА № 3. Защищенное или тайное многостороннее вычисление.**
**ТЕМА № 4. Гомоморфное шифрование**
**ТЕМА № 5. Шифрование с сохранением порядка.**
**ТЕМА № 6. Proxy re-encryption.**

2. Выполнение практического задания

Распределение весов по модуля и формам контроля

| | Вес формы текущего контроля в результирующей оценке текущего контроля | | Вес формы промежуточного контроля и результирующей оценки текущего контроля в итоговой оценке промежуточного контроля | | Вес итоговых оценок промежуточных контролей в результирующей оценке промежуточного контроля | Вес оценки результирующей оценки промежуточных контролей и оценки итогового контроля в результирующей оценке итогового контроля |
|---|---|---|---|---|---|---|
| **Вид учебной работы/контроля** | **М1**[1] | **М2** | **М1** | **М2** | | |
| Контрольная работа | | | | 1 | | |
| Письменные домашние задания | | 1 | | | | |
| 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 результирующей оценки промежуточных контролей в результирующей оценке итогового контроля | | | | | | 0.4 |

1

| | | | | | | |
|---|---|---|---|---|---|---|
| **Экзамен/зачет (оценка итогового контроля)** | | | | | | 0.6 |
| | **Σ = 1** | **Σ = 1** | **Σ = 1** | **Σ = 1** | **Σ = 1** | **Σ = 1** |

**Рекомендуемая литература.**


1. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone “Handbook of Applied Cryptography” Published October 16, 1996 by CRC Press, 810 Pages
2. Bernard L. Menezes, Ravinder Kumar “Cryptography, Network Security, and Cyber Laws”, 1st edition (August 8, 2018)