

**Học phần:** An toàn và bảo mật hệ thống thông tin  
**Số tín chỉ:** 3  
**Mã học phần:** INT1303

**Lớp:** D21CNTT  
**Hệ đào tạo:** Đại học chính quy

(Các mục bị gạch sẽ không thi)

## **Chương 1: Tổng quan về an toàn và bảo mật hệ thống thông tin**

- 1.1. Khái quát về an toàn thông tin
  - 1.1.1. An toàn thông tin là gì?
  - 1.1.2. Sự cần thiết của an toàn thông tin
  - 1.1.3. Các thành phần của ATTT
- 1.2. Khái quát về an toàn hệ thống thông tin
  - 1.2.1. Các thành phần của hệ thống thông tin
  - 1.2.2. An toàn hệ thống thông tin là gì?
- 1.3. Các yêu cầu an toàn hệ thống thông tin
  - 1.3.1. Bí mật
  - 1.3.2. Toàn vẹn
  - 1.3.3. Sẵn dùng
- 1.4. Bảy vùng trong cơ sở hạ tầng CNTT và các mối đe dọa
  - 1.4.1. Bảy vùng trong cơ sở hạ tầng CNTT
  - 1.4.2. Các mối đe dọa và nguy cơ
- 1.5. Mô hình tổng quát đảm bảo an toàn hệ thống thông tin
  - 1.5.1. Giới thiệu
  - 1.5.2. Một số mô hình đảm bảo an toàn hệ thống thông tin

## **Chương 2: Các dạng tấn công và phần mềm độc hại**

- 2.1. Khái quát về mối đe dọa, điểm yếu, lỗ hổng và tấn công
  - 2.1.1. Khái niệm mối đe dọa, điểm yếu, lỗ hổng và tấn công
  - 2.1.2. Các dạng mối đe dọa thường gặp
  - 2.1.3. Các lỗ hổng thường gặp trong hệ điều hành và phần mềm ứng dụng
  - 2.1.4. Các loại tấn công
- ~~2.2. Các công cụ hỗ trợ tấn công~~
  - ~~2.2.1. Công cụ rà quét lỗ hổng, điểm yếu hệ thống~~
  - ~~2.2.2. Công cụ rà quét công dịch vụ~~
  - ~~2.2.3. Công cụ nghe lén~~
  - ~~2.2.4. Công cụ ghi phím gõ~~
- 2.3. Các dạng tấn công thường gặp
  - 2.3.1. Tấn công vào mật khẩu
  - 2.3.2. Tấn công bằng mã độc
  - 2.3.3. Tấn công từ chối dịch vụ
  - 2.3.4. Tấn công từ chối dịch vụ phân tán
  - 2.3.5. Tấn công giả mạo địa chỉ
  - 2.3.6. Tấn công nghe lén
  - 2.3.7. Tấn công kiểu người đứng giữa

- 2.3.8. Tấn công bằng bom thư và thư rác
- 2.3.9. Tấn công sử dụng các kỹ thuật xã hội
- 2.3.10. Tấn công pharming
- 2.3.11. Tấn công APT
- 2.4. Các dạng phần mềm độc hại
  - 2.4.1. Phân loại
  - 2.4.2. Mô tả các dạng phần mềm độc hại
  - 2.4.3. Phòng chống phần mềm độc hại

### **Chương 3: Đảm bảo an toàn thông tin dựa trên mã hóa**

- 3.1 Khái quát về mã hóa thông tin và ứng dụng
  - 3.1.1 Các khái niệm
  - 3.1.2 Các thành phần của một hệ mã hóa
  - 3.1.3 Lịch sử mã hóa
  - 3.1.4 Mã hóa dòng và mã hóa khối
  - 3.1.5 Ứng dụng của mã hóa
- 3.2 Các phương pháp mã hóa
- 3.3 Các giải thuật mã hóa
  - 3.3.1 Các giải thuật mã hóa khóa đối xứng
  - 3.3.2 Các giải thuật mã hóa khóa bất đối xứng
  - 3.3.3 Các hàm băm
- 3.4 Chữ ký số, chứng chỉ số và PKI
  - 3.4.1 Chữ ký số
  - 3.4.2 Chứng chỉ số
  - 3.4.3 PKI
- ~~3.5 Quản lý khóa và phân phối khóa~~
  - ~~3.5.1 Giới thiệu~~
  - ~~3.5.2 Phân phối khóa bí mật~~
  - ~~3.5.2 Phân phối khóa công khai~~
- 3.6 Một số giao thức đảm bảo an toàn thông tin dựa trên mã hóa
  - 3.6.1 SSL/TLS
  - ~~3.6.2 SET~~
  - 3.6.3 PGP

### **Chương 4: Các kỹ thuật và công nghệ đảm bảo an toàn thông tin**

- 4.1 Khái quát về các kỹ thuật và công nghệ đảm bảo ATTT
- 4.1 Kiểm soát truy cập
  - 4.1.1 Khái niệm kiểm soát truy cập
  - 4.1.2 Các biện pháp kiểm soát truy cập
  - 4.1.3 Một số công nghệ kiểm soát truy cập
- 4.2 Tường lửa
  - 4.2.1. Khái quát
  - 4.2.2. Các loại tường lửa
  - 4.2.3. Các kỹ thuật kiểm soát truy cập
  - 4.2.4. Các hạn chế của tường lửa
- 4.3 Các hệ thống phát hiện và ngăn chặn xâm nhập
  - 4.3.1 Giới thiệu
  - 4.3.2 Phân loại

#### 4.3.3 Các kỹ thuật phát hiện xâm nhập

### **Chương 5: Quản lý, chính sách và pháp luật an toàn thông tin**

#### 5.1 Quản lý an toàn thông tin

##### 5.1.1 Khái quát về quản lý ATTT

##### 5.1.2 Đánh giá rủi ro ATTT

##### 5.1.3 Phân tích chi tiết rủi ro ATTT

##### 5.1.4 Thực thi quản lý an toàn thông tin

#### 5.2 Các bộ chuẩn quản lý ATTT

##### 5.2.1. Giới thiệu

##### 5.2.2. Chu trình Plan-Do-Check-Act

#### 5.3 Pháp luật và chính sách ATTT

##### 5.3.1 Giới thiệu về pháp luật và chính sách an toàn thông tin

##### 5.3.2 Luật quốc tế về an toàn thông tin

##### 5.3.3 Luật Việt Nam về an toàn thông tin

#### ~~5.4 Vấn đề đạo đức an toàn thông tin~~