**Nội dung ôn tập môn học ATBM HTTT**

(Các mục bị gạch sẽ không thi)

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

* 1. Khái quát về an toàn thông tin
     1. An toàn thông tin là gì?

An toàn thông tin là việc bảo vệ chống truy nhập, sử dụng, tiết lộ, sửa đổi, hoặc phá hủy thông tin một cách trái phép

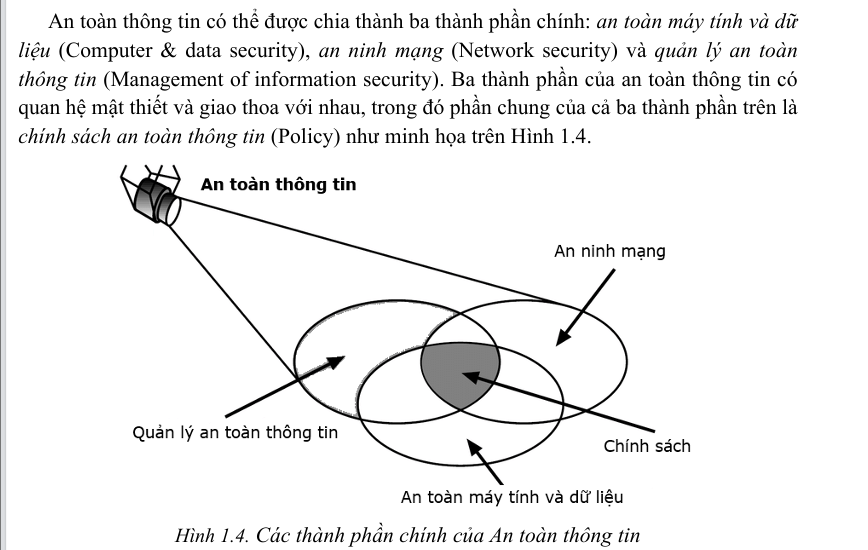
* + 1. Sự cần thiết của an toàn thông tin

An toàn thông tin hệ thống mạng và các thiết bị kết nối khác là rất cần thiết bởi 2 lý do:

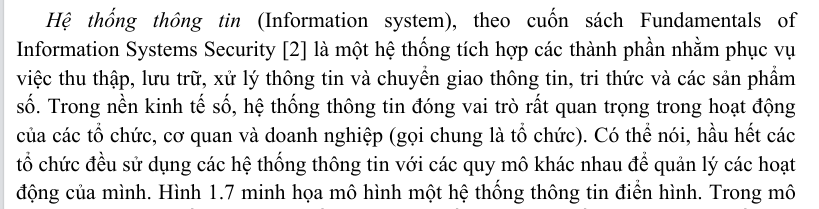
+ Số lượng các thiết bị có kết nối Internet tăng nhanh chóng, đặc biệt là các thiết bị thông minh, IoT

+ Sự bùng phát của các dạng phần mềm độc hại, các dạng tấn công mạng trên diện rộng và các nguy cơ gây mất an toàn thông tin. Việc đảm bảo an toàn thông tin không chỉ cần thiết đối với các cá nhân, tổ chức, cơ quan, doanh nghiệp mà còn là vấn đề cấp thiết đối với an ninh quốc gia. Hơn nữa, việc xây dựng các giải pháp an toàn thông tin chỉ thực sự hiệu quả khi được thực hiện bài bản, đồng bộ, đảm bảo cân bằng giữa tính an toàn, tính hữu dụng của hệ thống và chi phí đầu tư cho các biện pháp đảm bảo an toàn.

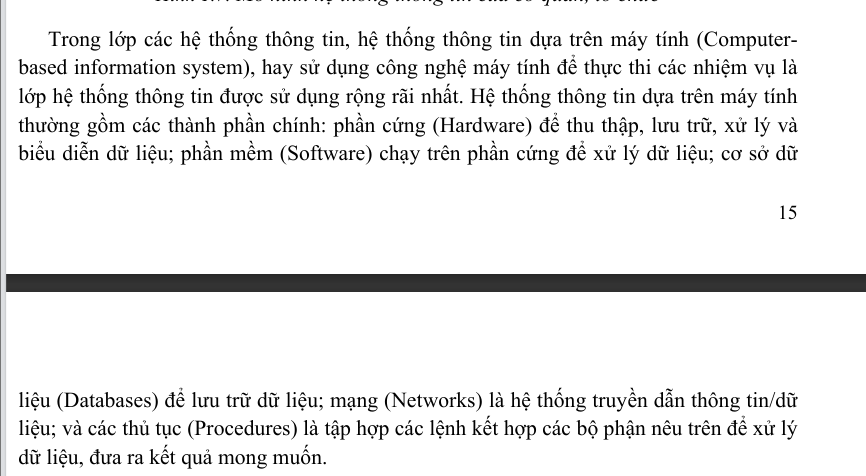
* + 1. Các thành phần của ATTT



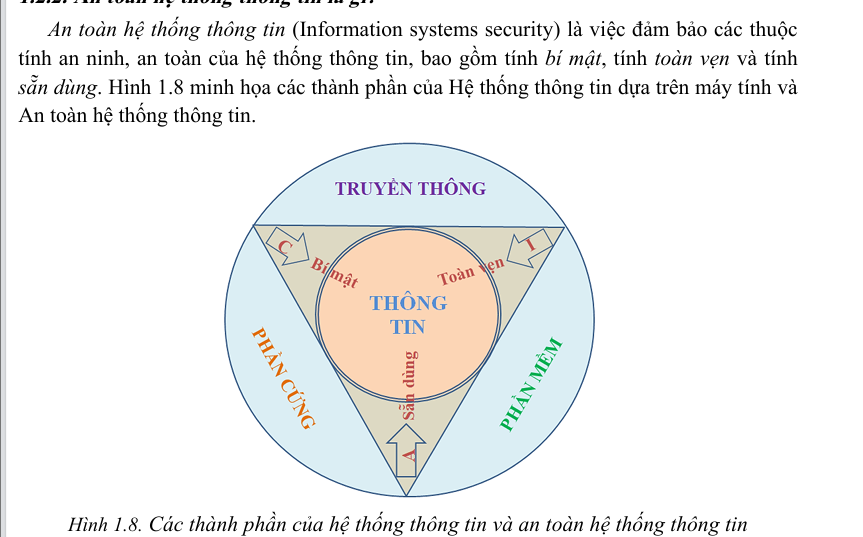
* 1. **Khái quát về an toàn hệ thống thông tin**



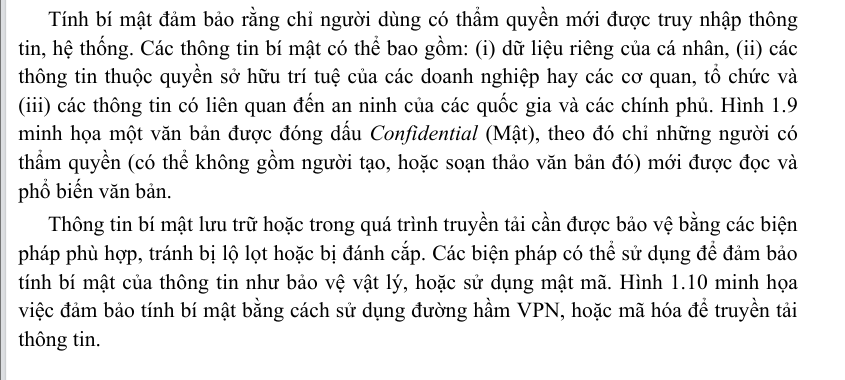
* + 1. **Các thành phần của hệ thống thông tin**



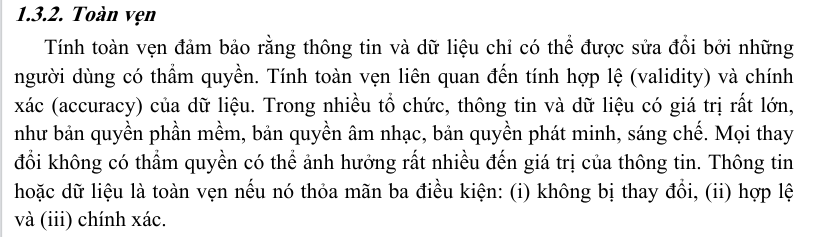
* + 1. An toàn hệ thống thông tin là gì?



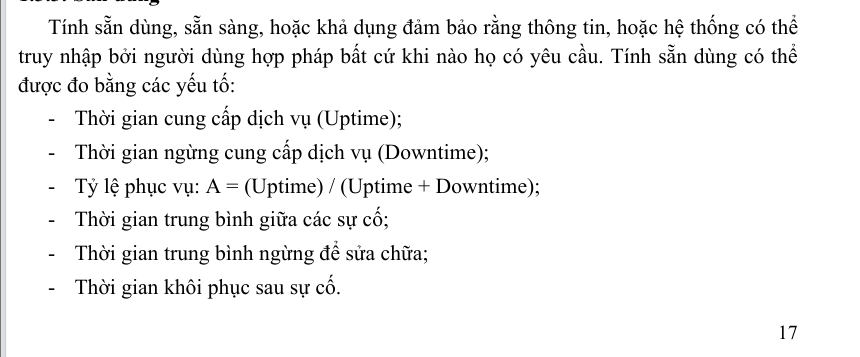
* 1. Các yêu cầu an toàn hệ thống thông tin
     1. Bí mật



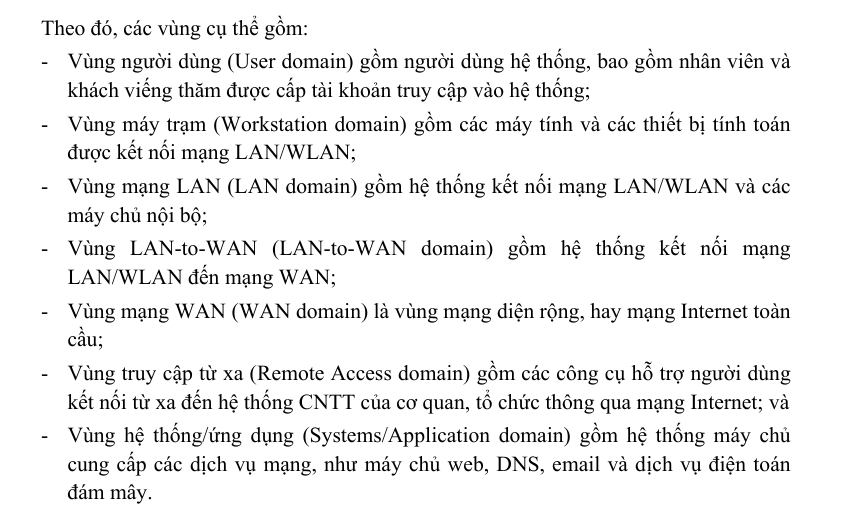
* + 1. Toàn vẹn



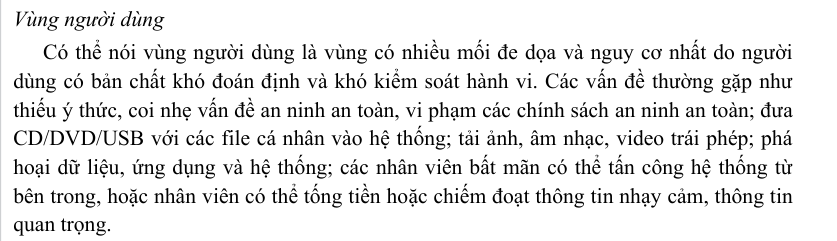
* + 1. Sẵn dùng

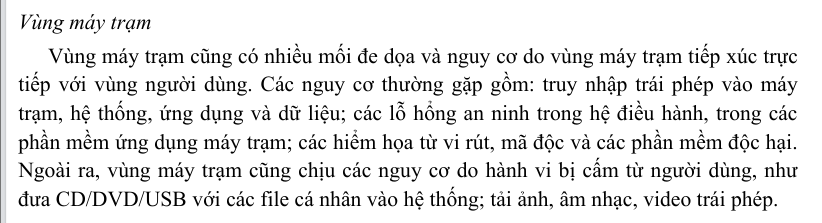


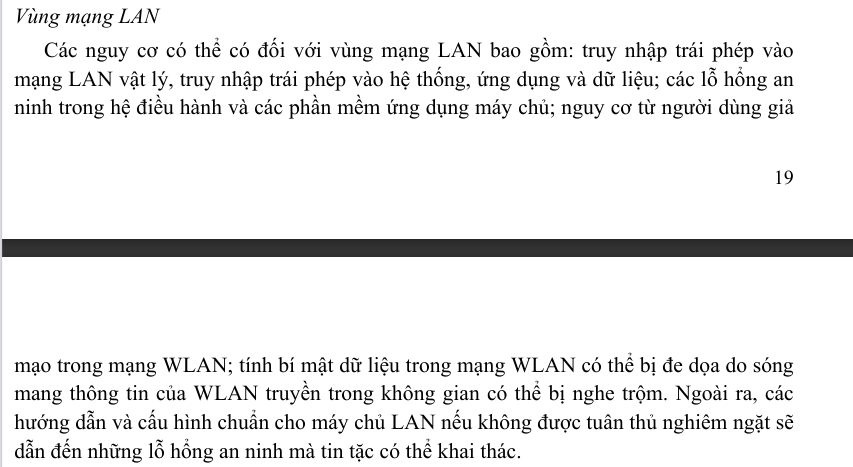
* 1. Bảy vùng trong cơ sở hạ tầng CNTT và các mối đe dọa
     1. Bảy vùng trong cơ sở hạ tầng CNTT

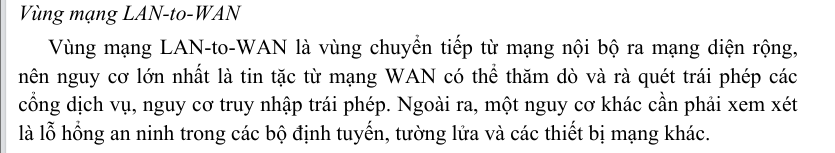


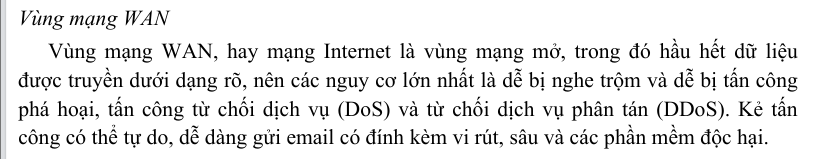
* + 1. Các mối đe dọa và nguy cơ

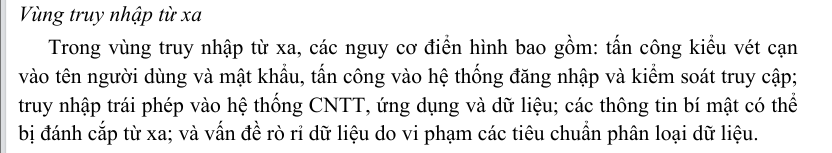


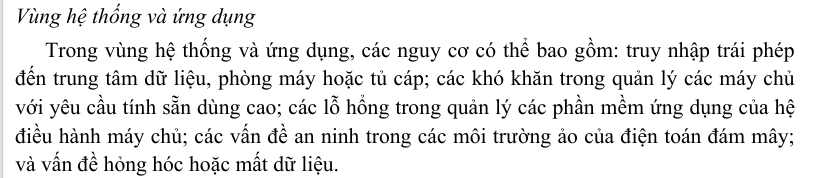




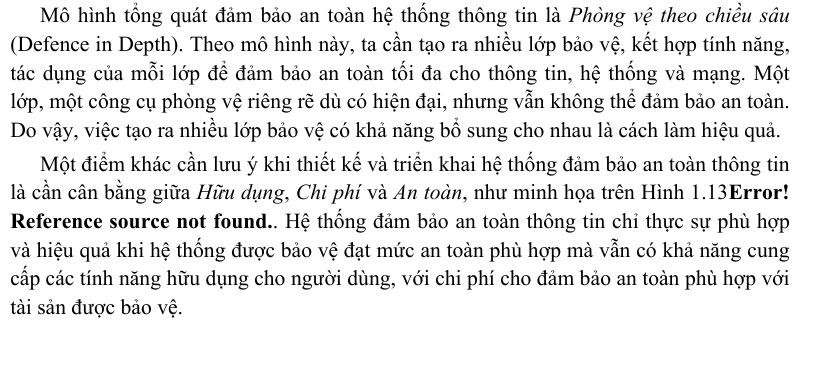








* 1. Mô hình tổng quát đảm bảo an toàn hệ thống thông tin
     1. Giới thiệu



* + 1. Một số mô hình đảm bảo an toàn hệ thống thông tin

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

* 1. Khái quát về mối đe dọa, điểm yếu, lỗ hổng và tấn công
     1. Khái niệm mối đe dọa, điểm yếu, lỗ hổng và tấn công
     2. Các dạng mối đe dọa thường gặp
     3. Các lỗ hổng thường gặp trong hệ điều hành và phần mềm ứng dụng
     4. Các loại tấn công
  2. ~~Các công cụ hỗ trợ tấn công~~
     1. ~~Công cụ rà quét lỗ hổng, điểm yếu hệ thống~~
     2. ~~Công cụ rà quét cổng dịch vụ~~
     3. ~~Công cụ nghe lén~~
     4. ~~Công cụ ghi phím gõ~~
  3. Các dạng tấn công thường gặp
     1. Tấn công vào mật khẩu
     2. Tấn công bằng mã độc
     3. Tấn công từ chối dịch vụ
     4. Tấn công từ chối dịch vụ phân tán
     5. Tấn công giả mạo địa chỉ
     6. Tấn công nghe lén
     7. Tấn công kiểu người đứng giữa
     8. Tấn công bằng bom thư và thư rác
     9. Tấn công sử dụng các kỹ thuật xã hội
     10. Tấn công pharming
     11. Tấn công APT
  4. Các dạng phần mềm độc hại
     1. Phân loại
     2. Mô tả các dạng phần mềm độc hại
     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~~