

Chương I

1

TỔNG QUAN VỀ AN TOÀN HỆ THỐNG THÔNG TIN

GV: Trần Thị Kim Chi

NỘI DUNG

1. Các khái niệm cơ bản
2. Các bước cơ bản trong bảo mật thông tin
3. Các bài toán an toàn thông tin cơ bản
4. Bài toán bảo mật : mã hóa và phong bì số
5. Bài toán chứng thực và toàn vẹn : chữ ký điện tử và mã chứng thực
6. Một ví dụ : giao thức bảo mật email PGP

Những khái niệm cơ bản

- Dữ liệu và thông tin
- Hệ thống thông tin
- Bảo mật hệ thống thông tin
- Những yêu cầu bảo mật hệ thống thông tin
- Mục tiêu của bảo mật

Dữ liệu và thông tin

- **Dữ liệu (Data)** là các giá trị của thông tin định lượng hoặc định tính của các sự vật, hiện tượng trong cuộc sống. Trong tin học, dữ liệu được dùng như một cách biểu diễn hình thức hoá của thông tin về các sự kiện, hiện tượng thích ứng với các yêu cầu truyền nhận, thể hiện và xử lý bằng máy tính.
- **Thông tin (Information)** là dữ liệu đã được xử lý, phân tích, tổ chức nhằm mục đích hiểu rõ hơn sự vật, sự việc, hiện tượng theo một góc độ nhất định.

An Toàn thông tin là gì?

Tổng quan

Mình đã biết
hết những gì
bạn chúng trao
đổi với nhau.



3

Bí mật



An Toàn thông tin là gì?



An Toàn thông tin là gì?



An Toàn thông tin là gì?

- An toàn thông tin bao hàm một lĩnh vực rộng lớn các hoạt động trong một tổ chức. Nó bao gồm cả những sản phẩm và những quy trình nhằm ngăn chặn truy cập trái phép, hiệu chỉnh, xóa thông tin, kiến thức, dữ liệu.
- Mục đích là đảm bảo một môi trường thông tin tin cậy , an toàn và trong sạch cho mọi thành viên và tổ chức trong xã hội

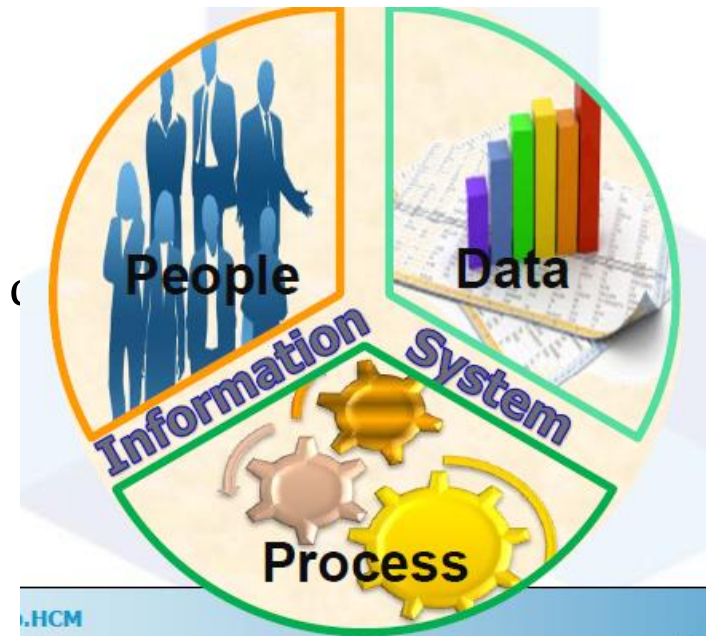
Hệ thống thông tin

- ***Hệ thống thông tin (Information Systems)***

- là một hệ thống gồm con người, dữ liệu và những hoạt động xử lý dữ liệu và thông tin trong một tổ chức.

- **Tài sản của hệ thống bao gồm:**

- ✓ Phần cứng
- ✓ Phần mềm
- ✓ Dữ liệu
- ✓ Các truyền thông giữa các máy tính
- ✓ Môi trường làm việc
- ✓ Con người



Bảo mật hệ thống thông tin

- ***Bảo mật hệ thống thông tin (Information Systems Security)***
 - Bao hàm một lĩnh vực rộng lớn các hoạt động trong một tổ chức.
 - Nó bao gồm cả những sản phẩm và những quy trình nhằm ngăn chặn truy cập trái phép, hiệu chỉnh, xóa, phá hủy, làm lộ và làm gián đoạn thông tin và hoạt động của hệ thống một cách trái phép.