TRƯỜNG ĐẠI HỌC KỸ THUẬT - CÔNG NGHỆ CẦN THƠ
KHOA CÔNG NGHỆ THÔNG TIN

AN TOÀN VÀ BẢO MẬT THÔNG TIN

CẦN THƠ, 2025

Thông tin môn học

- Mã số: TT021
- Số tín chỉ: 3 (30 LT, 30 TH)
- Bộ môn phụ trách: Hệ thống thông tin

GIỚI THIỆU MÔN HỌC

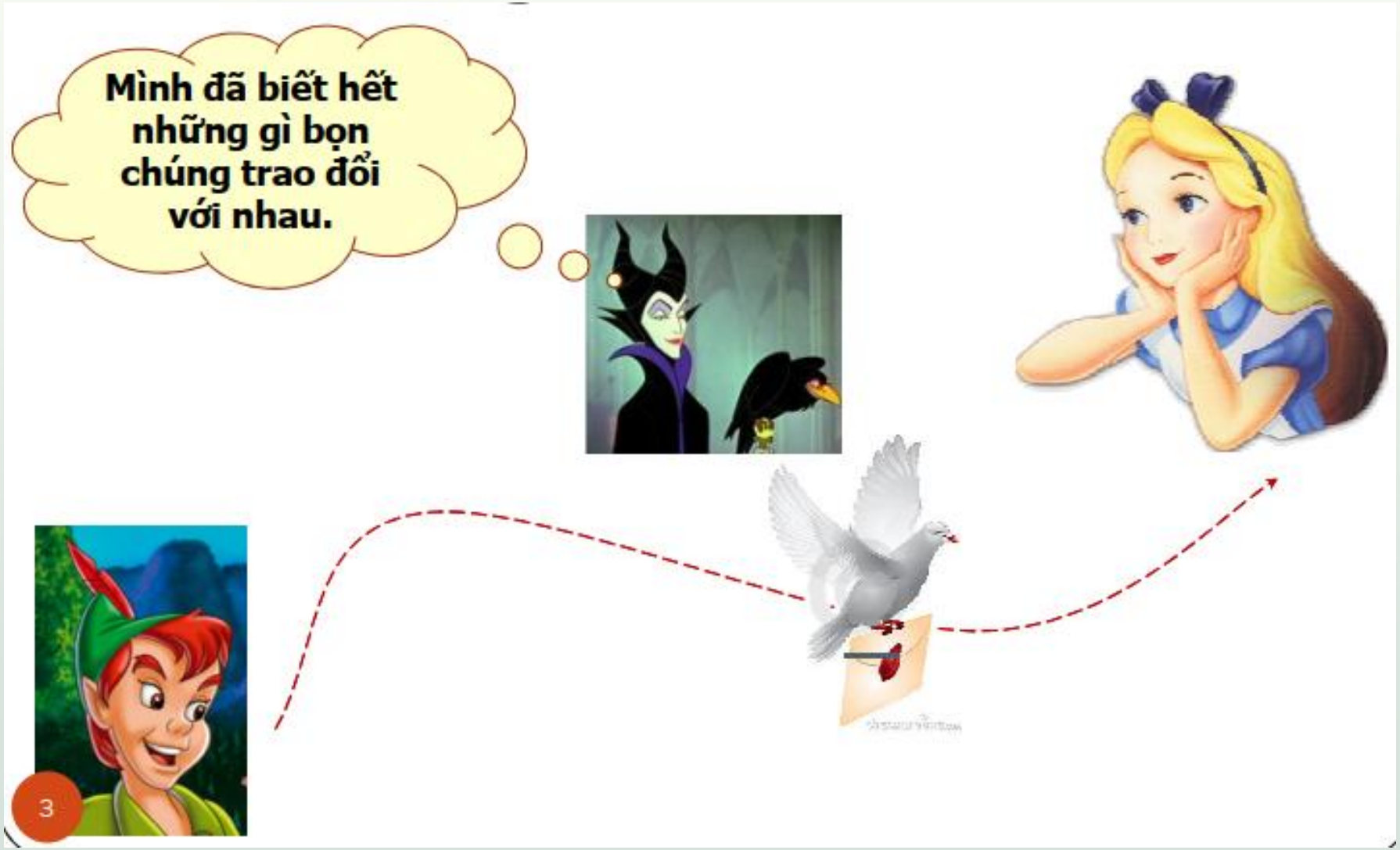
- Phương pháp nghiên cứu: lý thuyết, thực hành
- Thời gian
  - Lý thuyết: 10 tuần (30 tiết)
  - Thực hành: 6 tuần x 2 nhóm (30 tiết)
  - Lưu ý: vắng quá 20% số buổi sẽ cấm thi (3 buổi)
- Đánh giá môn học:
  - Giữa kỳ: 40% (30% báo cáo/trắc nghiệm + 10% điểm danh)
  - Cuối kỳ: 60% (40 câu/50 phút)

Phương pháp giảng dạy

- Lý thuyết:
  - Thuyết trình + Minh họa bằng chương trình máy tính
  - Đặt vấn đề + thảo luận
  - **Làm bài tập nhóm (nếu báo cáo)**

Tại sao phải học AT & BMTT

❖ Tình hướng 1



Tại sao phải học AT & BMTT

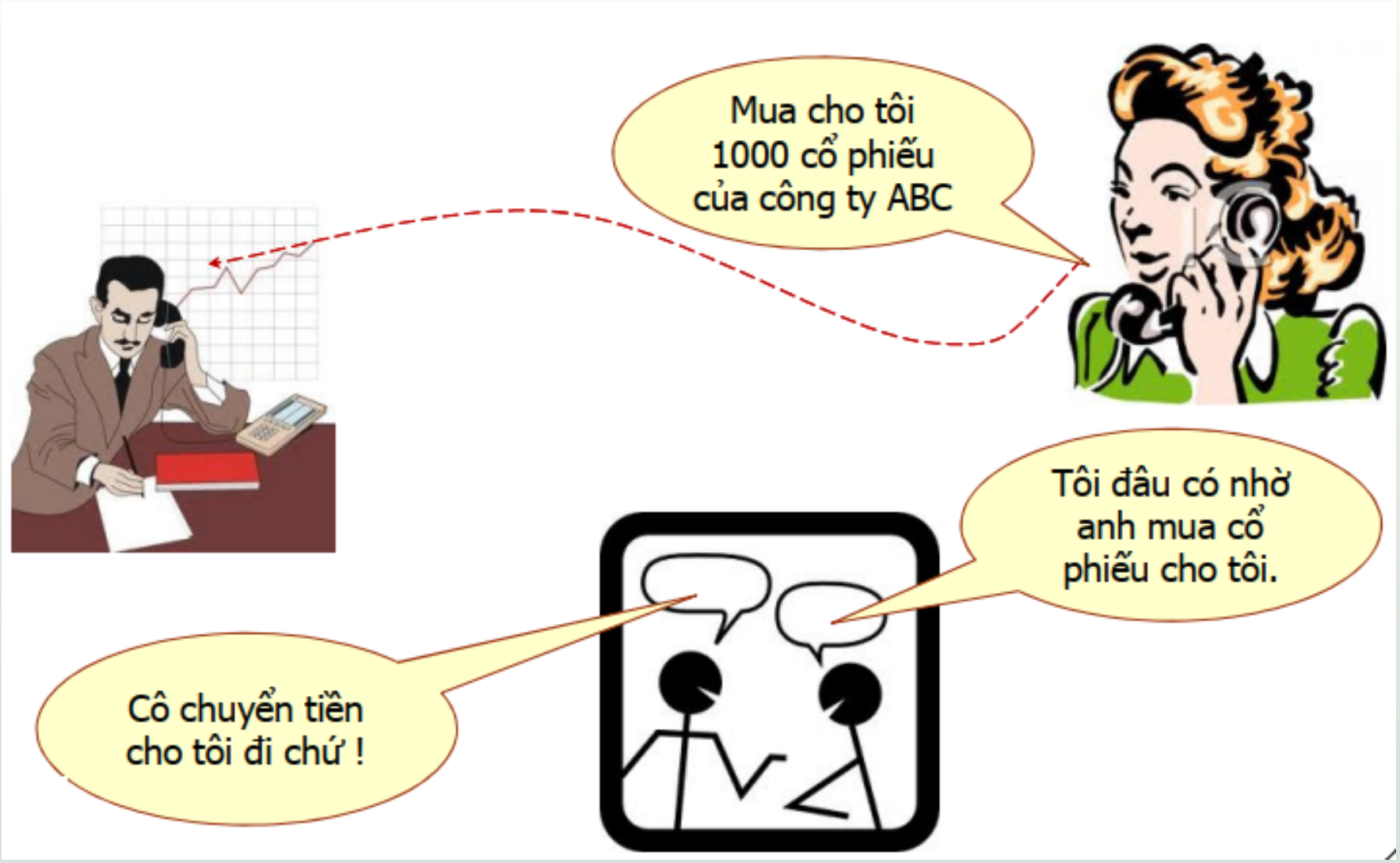
❖ Tình huống 2

Tại sao phải học AT & BMTT

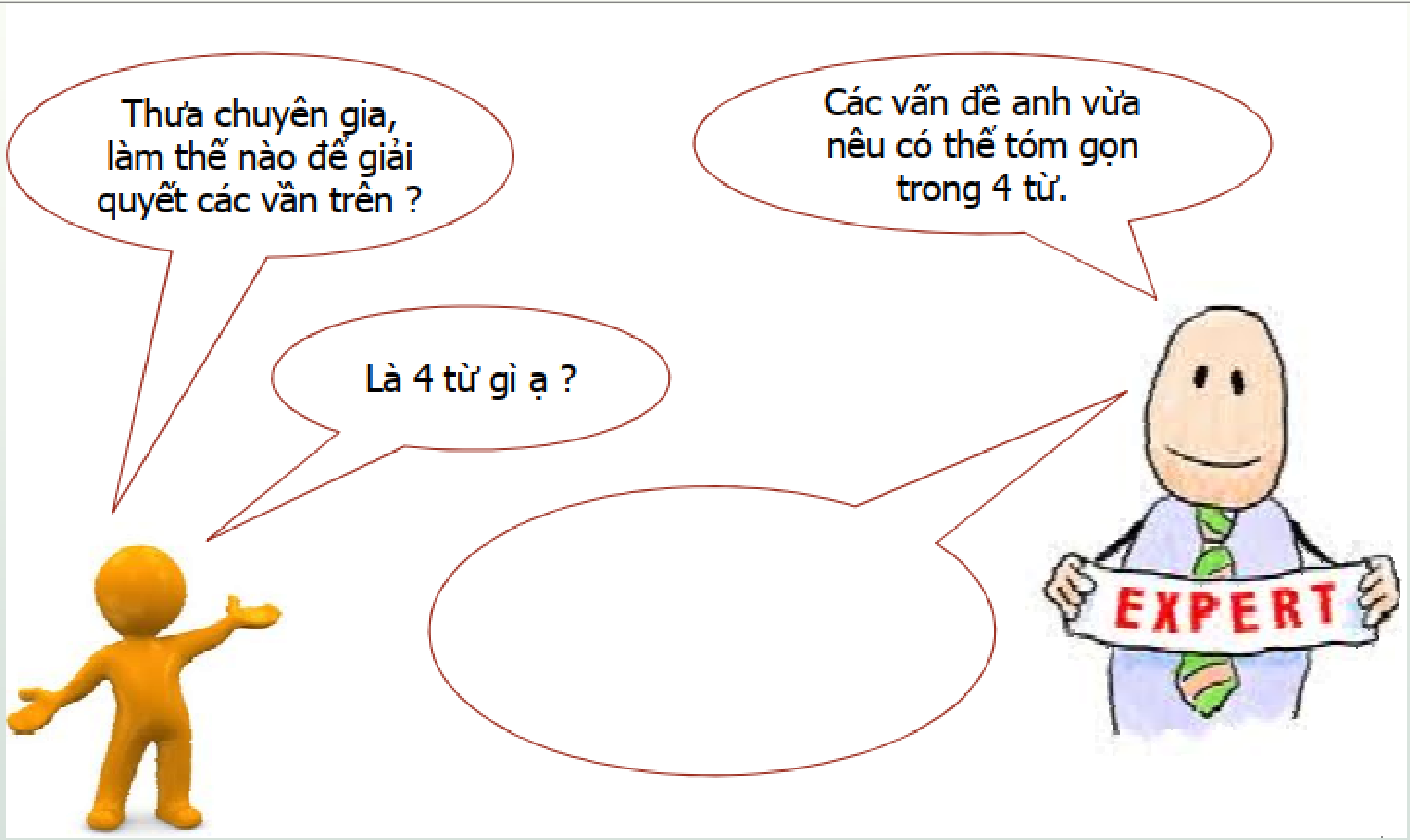
❖ Tình huống 3

Tại sao phải học AT & BMTT

❖ Tình huống 4



Tại sao phải học AT & BMTT



Mục tiêu môn học

- Biết
  - Các khái niệm cơ bản về bảo mật thông tin
- Hiểu và vận dụng:
  - Mật mã và ứng dụng của nó trong AT&BMTT
    - Các hệ mật mã
    - Các giải thuật được sử dụng
  - Chữ ký điện tử
  - Chứng thực người dùng và trao đổi khóa

Liên hệ Giảng viên

- Nguyễn Trung Kiên
- ntkien@ctuet.edu.vn
- Phòng giảng viên Khoa CNTT

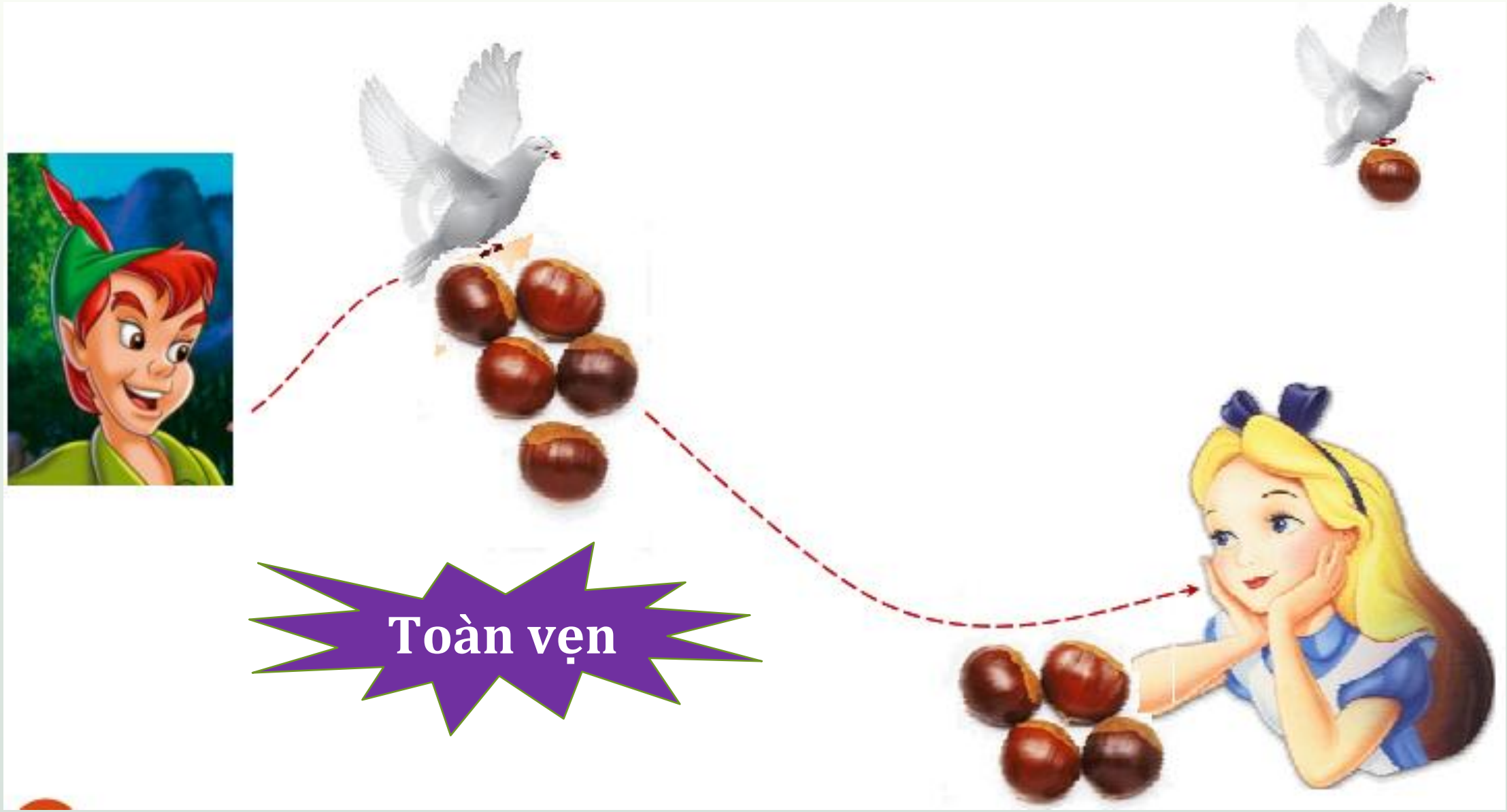
Tài liệu tham khảo

- TS Đào Thế Long. *Giáo trình an toàn và bảo mật thông tin*. SEI (series in software engineering) Đại học Mở TP HCM, 2010.
- Mark Rhodes-Ousley. *Information Security The Complete Reference*. McGraw-Hill Osborne Media, 2013.
- Jason Andress. *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*. Syngress, 2011.
- Jason Andress. *The Basics of Information Security*. 2011. Elsevier Inc.
- William Stallings. Network security essentials: *Applications and Standards*. 2011. Prentice Hall, 4th edition.

Chương 1
Tổng quan
An toàn và bảo mật thông tin

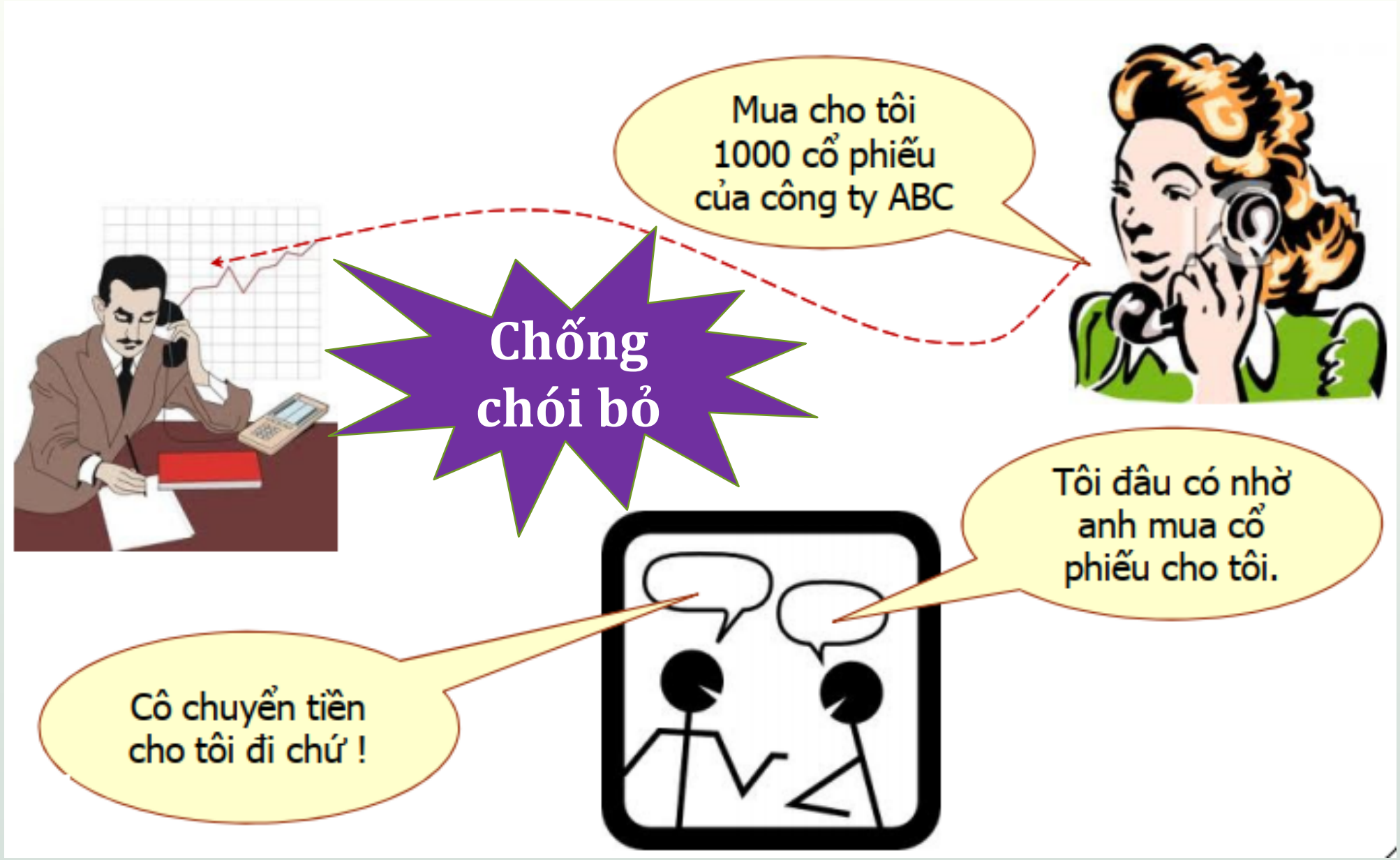
Tổng quan An toàn và bảo mật thông tin

Tổng quan An toàn và bảo mật thông tin



Tổng quan An toàn và bảo mật thông tin

Tổng quan An toàn và bảo mật thông tin



Tổng quan An toàn và bảo mật thông tin

- Nội dung của an toàn và bảo mật thông tin:
  - Khi nhu cầu trao đổi thông tin dữ liệu ngày càng lớn và đa dạng. Bảo vệ an toàn thông tin dữ liệu là một chủ đề rộng, có liên quan đến nhiều lĩnh vực.

Tổng quan An toàn và bảo mật thông tin

- Các phương pháp bảo vệ ATTT dữ liệu có thể được quy tụ vào ba nhóm sau:
  - Bảo vệ an toàn thông tin bằng các biện pháp hành chính.
  - Bảo vệ an toàn thông tin bằng các biện pháp kỹ thuật (phần cứng).
  - Bảo vệ an toàn thông tin bằng các biện pháp thuật toán (phần mềm).

=> Ba nhóm trên có thể được ứng dụng riêng rẽ hoặc phối kết hợp

Tổng quan An toàn và bảo mật thông tin

- Môi trường khó bảo vệ an toàn thông tin nhất và cũng là môi trường đối phương dễ xâm nhập nhất đó là môi trường mạng và truyền tin.
- Biện pháp hiệu quả nhất và kinh tế nhất hiện nay trên mạng truyền tin và mạng máy tính là biện pháp thuật toán.

Tổng quan An toàn và bảo mật thông tin

- An toàn thông tin bao gồm các nội dung sau:
  - **Tính bí mật:** tính kín đáo riêng tư của thông tin
  - **Tính xác thực của thông tin**, bao gồm xác thực đối tác (bài toán nhận danh), xác thực thông tin trao đổi.
  - **Tính trách nhiệm:** đảm bảo người gửi thông tin không thể thoái thác trách nhiệm về thông tin mà mình đã gửi

Tổng quan An toàn và bảo mật thông tin

- Để đảm bảo ATTT dữ liệu trên đường truyền tin và trên mạng dự đoán trước các khả năng:
  - không an toàn,
  - khả năng xâm phạm,
  - các sự cố rủi ro có thể xảy ra đối với thông tin dữ liệu được lưu trữ và trao đổi trên đường truyền tin cũng như trên mạng.
- Xác định càng chính xác các nguy cơ nói trên thì càng quyết định được tốt các giải pháp để giảm thiểu các thiệt hại.

Tổng quan An toàn và bảo mật thông tin

- Có hai loại hành vi xâm phạm thông tin:
  - Xâm phạm thụ động: liên quan đến việc nghe lén hoặc quan sát thông tin được truyền đi
    - **Tách nội dung thông điệp**: thu các thông tin nhạy cảm trong thư điện tử hay trong các tập tin truyền đi.
    - **Phân tích đường truyền**: thông tin nhạy cảm có thể được che dấu bằng mã hóa, nhưng đối thủ có thể xác định vị trí các thực thể và quan sát tần suất và độ dài của thông điệp để rút trích bản chất của thông điệp

Tổng quan An toàn và bảo mật thông tin

=>Xâm phạm thụ động **khó phát hiện** vì không có ảnh hưởng đến tài nguyên và thao tác của hệ thống -> tập trung phòng chống

Tổng quan An toàn và bảo mật thông tin

- Có hai loại hành vi xâm phạm thông tin:
  - Xâm phạm chủ động: liên quan đến việc thay đổi dữ liệu hoặc tạo dữ liệu sai
    - **Giả mạo**: thực hiện các thao tác theo sau một chứng thực hợp lệ để sử dụng các quyền của người dùng hợp lệ cho các thao tác "không hợp lệ" trong hệ thống.
    - **Làm lại (replay)**: truyền lại các gói tin của lần chứng thực hợp lệ của quá khứ cho các lần chứng thực trong tương lai.

Tổng quan An toàn và bảo mật thông tin

- **Thay đổi thông điệp**: một phần hoặc toàn bộ thông tin hợp pháp bị thay thế bằng các thông tin giả mạo nhằm thực hiện các tác vụ không cho phép.
- **Từ chối dịch vụ (denial of service)**: ngăn chặn hay gây ức chế việc sử dụng và quản lý thông thường của các thiết bị truyền thông.

=>Dễ phát hiện nhưng khó ngăn chặn

Các chiến lượt an toàn hệ thống

- **Giới hạn quyền hạn tối thiểu (Last Privilege):**
  - Đây là chiến lược cơ bản nhất theo nguyên tắc này bất kỳ một đối tượng nào cùng chỉ có những quyền hạn nhất định đối với tài nguyên mạng, khi thâm nhập vào mạng đối tượng đó chỉ được sử dụng một số tài nguyên nhất định.
- **Bảo vệ theo chiều sâu (Defence In Depth):**
  - Nguyên tắc này nhắc nhở chúng ta: Không nên dựa vào một chế độ an toàn nào dù cho chúng rất mạnh, mà nên tạo nhiều cơ chế an toàn để tương hỗ lẫn nhau.

Các chiến lược an toàn hệ thống

- **Nút thắt (Choke Point) :**
  - Tạo ra một "cửa khẩu" hẹp, và chỉ cho phép thông tin đi vào hệ thống của mình bằng con đường duy nhất chính là "cửa khẩu" này.
- **Điểm nối yếu nhất (Weakest Link) :**
  - Chiến lược này dựa trên nguyên tắc: "Một dây xích chỉ chắc tại mắt duy nhất, một bức tường chỉ cứng tại điểm yếu nhất"
  - Kẻ phá hoại thường tìm những chỗ yếu nhất của hệ thống để tấn công, do đó ta cần phải gia cố các yếu điểm của hệ thống.

Các chiến lượt an toàn hệ thống

- **Tính toàn cục:**
  - Các hệ thống an toàn đòi hỏi phải có tính toàn cục của các hệ thống cục bộ. Nếu có một kẻ nào đó có thể bẻ gãy một cơ chế an toàn thì chúng có thể thành công bằng cách tấn công hệ thống tự do của ai đó và sau đó tấn công hệ thống từ nội bộ bên trong.
- **Tính đa dạng bảo vệ:**
  - Cần phải sử dụng nhiều biện pháp bảo vệ khác nhau cho hệ thống khác nhau, nếu không có kẻ tấn công vào được một hệ thống thì chúng cũng dễ dàng tấn công vào các hệ thống khác

Các mức bảo vệ trên mạng

❖ Quyền truy nhập

- ➢ Lớp bảo vệ trong cùng là quyền truy nhập nhằm kiểm soát các tài nguyên của mạng và quyền hạn trên tài nguyên đó. Dĩ nhiên là kiểm soát được các cấu trúc dữ liệu càng chi tiết càng tốt. Hiện tại việc kiểm soát thường ở mức tệp

Các mức bảo vệ trên mạng

- **Đăng ký tên /mật khẩu.**
  - Thực ra đây cũng là kiểm soát quyền truy nhập, nhưng không phải truy nhập ở mức thông tin mà ở mức hệ thống. Đây là phương pháp bảo vệ phổ biến nhất vì nó đơn giản ít phí tổn và cũng rất hiệu quả.
  - Về lý thuyết nếu mọi người đều giữ kín được mật khẩu và tên đăng ký của mình thì sẽ không xảy ra các truy nhập trái phép. Song điều đó khó đảm bảo trong thực tế vì nhiều nguyên nhân rất đời thường làm giảm hiệu quả của lớp bảo vệ này.

Các mức bảo vệ trên mạng

❖ Mã hoá dữ liệu

- ➢ Để bảo mật thông tin trên đường truyền người ta sử dụng các phương pháp mã hoá. Dữ liệu bị biến đổi từ dạng nhận thức được sang dạng không nhận thức được theo một thuật toán nào đó và sẽ được biến đổi ngược lại ở trạm nhận (giải mã). Đây là lớp bảo vệ thông tin rất quan trọng

Các mức bảo vệ trên mạng

- **Bảo vệ vật lý**
  - Ngăn cản các truy nhập vật lý vào hệ thống. Thường dùng các biện pháp truyền thống như ngăn cấm tuyệt đối người không phận sự vào phòng đặt máy mạng, dùng ổ khoá trên máy tính hoặc các máy trạm không có ổ mềm.
- **Tường lửa**
  - Ngăn chặn thâm nhập trái phép và lọc bỏ các gói tin không muốn gửi hoặc nhận vì các lý do nào đó để bảo vệ một máy tính hoặc cả mạng nội bộ

Các mức bảo vệ trên mạng

❖ Quản trị mạng

- ➢ Công tác quản trị mạng máy tính phải được thực hiện một cách khoa học đảm bảo các yêu cầu sau:
  - Toàn bộ hệ thống hoạt động bình thường trong giờ làm việc.
  - Có hệ thống dự phòng khi có sự cố về phần cứng hoặc phần mềm xảy ra. Backup dữ liệu quan trọng theo định kỳ.
  - Bảo dưỡng mạng theo định kỳ.
  - Bảo mật dữ liệu, phân quyền truy cập, tổ chức nhóm làm việc trên mạng

THÔNG TIN

Thông tin

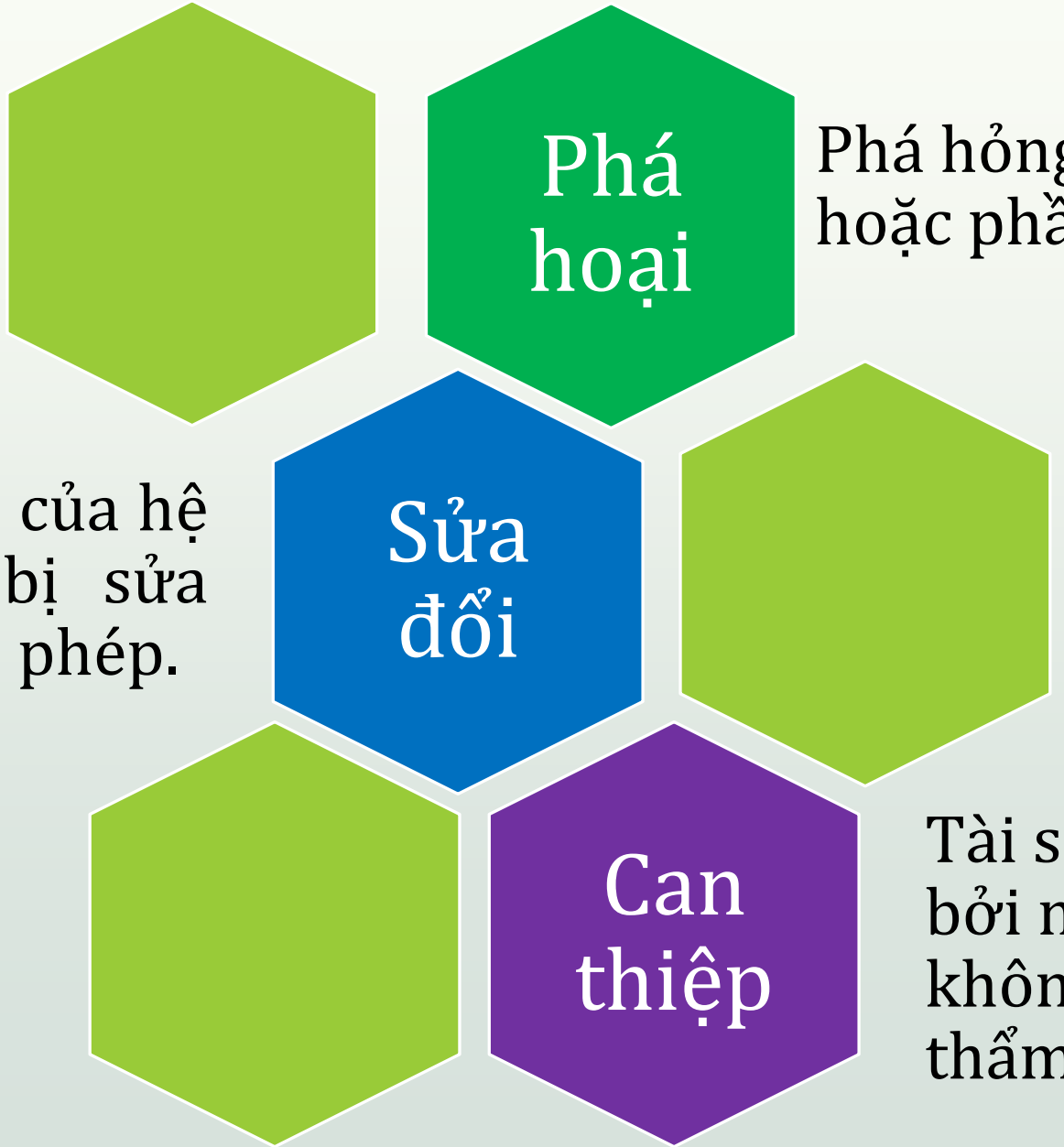
- Định nghĩa: thông tin là những tính chất xác định của vật chất mà con người (hoặc hệ thống kỹ thuật) nhận được từ thế giới vật chất bên ngoài hoặc từ những quá trình xảy ra trong bản thân nó.
- Thông tin tồn tại một cách khách quan, không phụ thuộc vào hệ thụ cảm

Tài nguyên thông tin:

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

Các mối đe doạ đối với một hệ thống thông tin và các biện pháp ngăn chặn

Các mối đe dọa đối với hệ thống thông tin

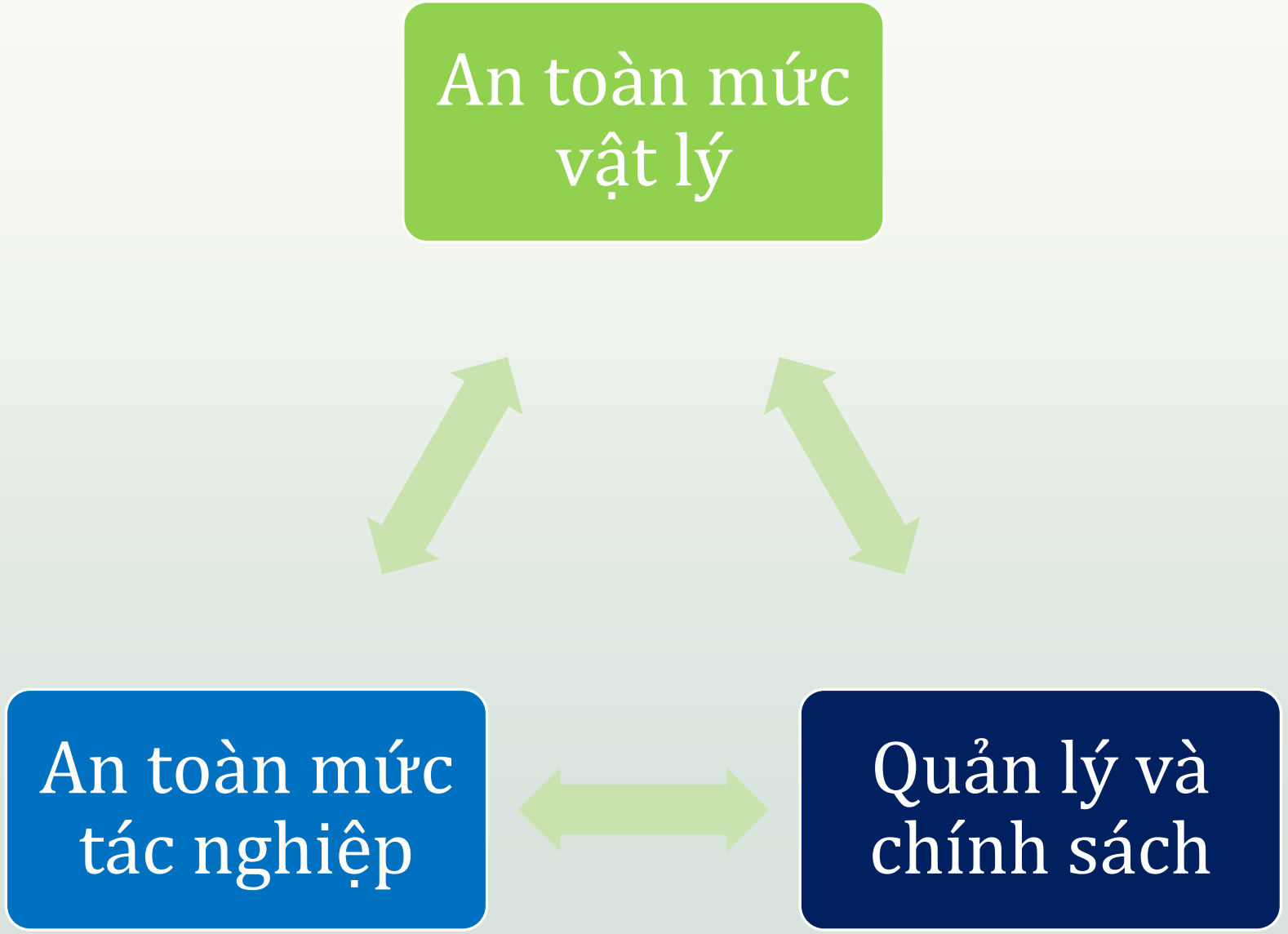


Phá hỏng thiết bị phần cứng hoặc phần mềm trên hệ thống

Tài sản của hệ thống bị sửa đổi trái phép.

Tài sản bị truy cập bởi những người không có thẩm quyền

Các thành phần chính của ATTT



An toàn vật lý

- An toàn ở mức vật lý là sự bảo vệ tài sản và thông tin của khỏi sự truy cập vật lý không hợp lệ .
- Đảm bảo an toàn mức vật lý tương đối dễ thực hiện.
- Biện pháp bảo vệ đầu tiên là làm sao cho vị trí của tổ chức càng ít trở thành mục tiêu tấn công càng tốt .

An toàn vật lý

- Biện pháp bảo vệ thứ hai phát hiện và ngăn chặn các kẻ đột nhập hay kẻ trộm: camera , t/b chống trộm.
- Biện pháp bảo vệ thứ ba là khôi phục những dữ liệu hay hệ thống cực kỳ quan trọng bị trộm hay mất mát.

Thao tác an toàn

- Thao tác an toàn liên quan những gì mà một tổ chức cần thực hiện để đảm bảo một chính sách an toàn
- Thao tác này bao gồm cả hệ thống máy tính, mạng, hệ thống giao tiếp và quản lý thông tin.
- Do đó thao tác an toàn bao hàm một lãnh vự rộng lớn và vì bạn là một chuyên gia an toàn nên bạn phải quan tâm trực tiếp đến các lãnh vực này

Quy tình thao tác an toàn

- Kiểm soát truy cập
- Chứng thực
- An toàn mạng sau khi việc thiết lập mạng
- Các thao tác an toàn trên đây không liên quan đến việc bảo vệ ở mức vật lý và mức thiết kế

Quy tình thao tác an toàn

- Sự kết hợp của tất cả các quá trình, các chức năng và các chính sách bao gồm cả yếu tố con người và yếu tố kỹ thuật.
- Yếu tố con người tập trung vào các chính sách được thực thi trong tổ chức.
- Yếu tố kỹ thuật bao gồm các công cụ mà cài đặt vào hệ thống.

Phần mềm chống virus

- Virus máy tính là và vấn đề phiền toái nhất.
- Các phương thức chống virus mới ra đời cũng nhanh tương tự như sự xuất hiện của chúng.
- File chống virus được cập nhật mỗi hai tuần một lần hay lâu hơn. Nếu các file này cập nhật thường xuyên thì hệ thống có thể là tương đối an toàn.
- Phát hiện và diệt virus trực tuyến

Kiểm soát truy cập

- Kiểm soát truy cập bắt buộc
- Kiểm soát truy cập tự do
- Kiểm soát truy cập theo vai trò

Kiểm soát truy cập bắt buộc

- (MAC – Mandatory Access Control)
  - Cách truy cập tĩnh, sử dụng một tập các quyền truy cập được định nghĩa trước đối với các file trong hệ thống.
- DAC – Discretionary Access Control
  - Do chủ tài nguyên cấp quyền thiết lập một danh sách kiểm soát truy cập (ACL –Access Control List)

Kiểm soát truy cập theo vai trò

Kiểm soát truy cập theo vai trò (chức vụ)

(RBAC– Role Based Access Control) :

- Truy cập với quyền hạn được xác định trước trong hệ thống, quyền hạn này căn cứ trên chức vụ của người dùng trong tổ chức.

Chứng thực

- Chứng minh " Tôi chính là tôi chứ không phải ai khác" là một phần quan trọng trong ĐỊNH DANH và CHỨNG THỰC.
  - Ba yếu tố của chứng thực:
    - Cái bạn biết (Something you know)– Mật mã hay số PI
    - Cái bạn có (Something you have) – Một card thông minh hay một thiết bị chứng thực.
    - Cái bạn sở hữu (Something you are) – dấu vân tay hay võng mạc mắt của bạn

Chứng thực bằng sinh trắc học

- Nhận dạng cá nhân bằng các đặc điểm riêng biệt của từng cá thể.
- Hệ thống sinh trắc học gồm các thiết bị quét tay, quét võng mạc mắt, và sắp tới sẽ có thiết bị quét DNA.
- Để có thể truy cập vào tài nguyên thì bạn phải trải qua quá trình nhận dạng vật lý.

Kế hoạch khôi phục sau biến cố

- Một trong những vấn đề nhức đầu nhất mà các chuyên gia CNTT phải đối mặt.
- Tốn rất nhiều tiền để thực hiện việc kiểm tra, sao lưu, thiết lập hệ thống dự phòng để giữ cho hệ thống hoạt động liên tục.
- Hầu hết các công ty lớn đều đầu tư một số tiền lớn vào kế hoạch khôi phục bao gồm việc sao lưu dữ liệu hay những lập "điểm nóng".
- "Điểm nóng" là một nơi được thiết kế để cung cấp các dịch vụ nhanh chóng và thuận tiện nhất khi có sự cố xảy ra như hệ thống hay mạng bị sập.

Sơ lược về lịch sử mật mã học

- Là ngành khoa học có lịch sử khoảng 4000 năm.
- Các phương pháp mã hóa đơn giản đầu tiên mà loài người đã sử dụng là của người Ba Tư Cổ và người Do Thái Cổ.

Sơ lược về lịch sử mật mã học

- Có hai thời kỳ:
  - Thời kỳ tiền khoa học :Trước công nguyên đến 1949 mang tính nghệ thuật. Đánh dấu vào năm 1949 khi Claude Shanno đưa ra lý thuyết thông tin.
  - Đầu những năm 1970 là sự phát triển của các thuật toán mã hóa khối đầu tiên: Lucipher và DES.

Sơ lược về lịch sử mật mã học

- Các hệ mã khối vẫn tiếp tục được phát triển thay thế cho DES vào cuối thế kỷ 20 như IDEA, AES hoặc 3DES.
- Các hàm băm MD5 và SHA1.
- MD5 và SHA1 đã bị hack, các nhà mật mã học đã khuyến cáo sử dụng các hàm băm mạnh hơn (SHA-256, SHA-512) trong các ứng dụng

Vai trò của mật mã trong việc bảo mật thông tin

- Mật mã hay mã hóa dữ liệu (cryptography), là một công cụ cơ bản thiết yếu của bảo mật thông tin.
- Mật mã đáp ứng được các nhu cầu về:
  - Tính bảo mật (confidentiality)
  - Tính chứng thực (authentication)
  - Tính không từ chối (non-repudiation) của một hệ truyền tin

Phân loại các thuật toán mật mã

- Các thuật toán mã hóa khóa bí mật (hệ mã mật khóa bí mật hay khóa đối xứng SKC)
- Các thuật toán mã hóa khóa công khai (các hệ mã khóa công khai PKC).
- Các hệ mã khóa bất đối xứng (AKC).
- Các thuật toán tạo chữ ký số (DSA).
- Các hàm băm (Hash functions).


thank
you!