

Đề cương ôn tập môn “[ĐẢM BẢO VÀ AN TOÀN THÔNG TIN](#)”

I. Cấu trúc đề thi

Phần I: 3 điểm – 03 câu hỏi

Phần II: 4 điểm – 04 câu hỏi

Phần III: 03 điểm – 01 câu hỏi phân tích mô hình

II. Câu hỏi phần chính sách, chương trình đảm bảo an toàn và bảo mật hệ thống thông tin

Câu hỏi 1: Khác nhau giữa các nhóm chính sách: mức 1, mức 2, mức 3 đưa ra một chính sách mức 1 an toàn bảo mật hệ thống thông tin theo một mô hình công ty

Câu hỏi 2: Mục tiêu của an toàn bảo mật thông tin. Đưa ra ví dụ việc đảm bảo các mục tiêu của an toàn và bảo mật thông tin.

Câu hỏi 3: Ý nghĩa phân lớp tài sản. Ví dụ minh họa phân lớp tài sản thông tin

Câu hỏi 4: Ý nghĩa điều khiển truy xuất, các vấn đề trong quản lý truy xuất người dùng

Câu hỏi 5: Ý nghĩa bảo mật vật lý, ví dụ chính sách bảo mật vật lý

Câu hỏi 6: Ý nghĩa của phân tích nguy cơ, tiến trình phân tích quản lý nguy cơ

Câu hỏi 7: Ý nghĩa kế hoạch công việc liên tục, sự liên quan của quá trình phân tích tác động công việc và các bước

Câu hỏi 8: Nêu lý do của vì sao phải thiết lập chính sách, tiêu chuẩn, chỉ dẫn về an toàn và đảm bảo thông tin trong doanh nghiệp.

Câu hỏi 9: Khác nhau giữa chính sách, tiêu chuẩn, chỉ dẫn. Đưa ra ví dụ minh chứng

Câu hỏi 10: Sự tương ứng của phân tích nguy cơ và quá trình phát triển hệ thống? Vòng đời của bảo mật thông tin?

III. Câu hỏi về phần kỹ thuật liên quan đến an toàn và bảo mật hệ thống thông tin

Câu hỏi 1: Nêu một số thuật toán mã hoá cổ điển, phân tích khả năng áp dụng mô hình cho mã hoá dữ liệu lưu trữ và mã hoá dữ liệu trên đường truyền.

Câu hỏi 2: Khác nhau giữa mã hoá cổ điển và các hàm băm. Nguyên lý của hàm băm, khả năng sử dụng hàm băm trong bảo vệ dữ liệu và các hệ thống ứng dụng

Câu hỏi 3: Cơ sở của mã hoá công khai RSA, phân tích khả năng sử dụng mã hoá RSA để lưu trữ dữ liệu trên hệ thống máy tính, truyền dữ liệu trên mạng máy tính.

Câu hỏi 4: Phân tích sự khác biệt mã hóa cổ điển và mã công khai, khả năng kết hợp giữa hai loại khóa trong truyền tin?

Câu hỏi 5: Giới thiệu về mã hóa ECC nguyên lý và ứng dụng.

Câu hỏi 6: Khác biệt và tương đồng giữa mã hóa cổ điển và mã hóa DES, AES?. Ứng dụng của DES, AES trong thực tế.

Câu hỏi 7: Trình bày mô hình chữ ký số. Sự cần thiết của triển khai mô hình chữ ký số trong giao dịch điện tử ở Việt Nam. Trình bày hiểu biết về hiện trạng mô hình chữ ký số ở Việt Nam.

Câu hỏi 8: Nguyên lý, khả năng, phương thức phòng chống với các phương thức tấn công mạng máy tính: Port scanning attack, Avesdropping attack, IP spoofing attack

Câu hỏi 9: Nguyên lý, khả năng, phương thức phòng chống với các phương thức tấn công mạng máy tính: Hijacking attack, Replay attack, Man-in-the-middle attack

Câu hỏi 10: Tấn công SQL injection, tràn bộ đệm, chéo trang – cross page attack? Giải pháp phòng chống?

Câu hỏi 11: Tấn công DoS, DDoS nguyên lý và khả năng phòng chống?

Câu hỏi 12: Khác nhau giữa virus, worm, trojan, back door.

Câu hỏi 13: Khả năng bảo vệ hệ thống của trình quét virus và firewall

Câu hỏi 14: IPSec, VPN khả năng bảo vệ thông tin trên đường truyền

IV. Câu hỏi về phân tích mô hình đảm bảo và an toàn hệ thống thông tin

Ví dụ một mô hình: Cho mô hình đào tạo tính chỉ

- Lưu thông tin đào tạo
- Lưu thông tin về sinh viên
- Lưu thông tin về điểm

Mô hình xử lý công việc

- Phòng đào tạo thực hiện lên kế hoạch và chương trình đào tạo (các môn học, lớp môn học, thời khóa biểu)

- Phòng đào tạo tổng hợp về thông tin đào tạo và quyết định về cảnh cáo, ..., thực hiện việc in điểm cuối khóa và quyết định về ra trường
- Giáo viên thực hiện môn học nhập điểm
- Sinh viên đăng ký môn học, xem điểm cá nhân

Mô hình triển khai hệ thống web

- Lưu điểm và kiểm soát điểm, nhập điểm, trên hệ thống mạng nội bộ học viện
- Sinh viên đăng ký môn học thông qua mạng internet và đồng bộ về mạng nội bộ
- Điểm, các kết quả được xử lý trên hệ thống mạng nội bộ sau đó được đồng bộ lên mạng internet để thông báo cho sinh viên

Câu hỏi:

- + Phân tích những nguy cơ với hệ thống
- + Những chính sách và tiêu chuẩn nào nên được đề xuất với hệ thống
- + Những tiêu chuẩn kỹ thuật về lập trình nào các hệ thống trang web cần phải được đảm bảo