

TP. Hồ Chí Minh, ngày 28 tháng 2 năm 2024

ĐỀ CƯƠNG MÔN HỌC

AN TOÀN THÔNG TIN TRONG KINH DOANH

A. THÔNG TIN CHUNG VỀ MÔN HỌC

- 1. Tên môn học (tiếng Việt) : AN TOÀN THÔNG TIN TRONG KINH DOANH**
- 2. Tên môn học (tiếng Anh) : INFORMATION SECURITY FOR BUSINESS**
- 3. Mã số môn học : DAT730**
- 4. Trình độ đào tạo : Đại học**
- 5. Ngành đào tạo áp dụng : Các ngành đào tạo bậc đại học**
- 6. Số tín chỉ : 03**
- 7. Phân bổ thời gian : 150 giờ**
 - **Trực tiếp : 45 giờ**
 - o *Lý thuyết* : 45 giờ
 - o *Thực hành* : 0 giờ
 - **Trực tuyến : không vượt quá 30% tổng thời gian giảng dạy của môn học.**
 - **Tự học, tự nghiên cứu : 105 giờ**
 - **Khác (ghi cụ thể) : 0 giờ**
- 8. Khoa quản lý môn học : Bộ môn Toán Kinh tế**
- 9. Môn học trước : Hệ quản trị cơ sở dữ liệu**
- 10. Mô tả môn học**

An toàn thông tin trong kinh doanh là môn học thuộc khối kiến thức ngành. Môn học giới thiệu tổng quan về an toàn bảo mật, các thành phần, nguyên tắc, cũng như các vấn đề về hacker, virus, thiên tai...; giới thiệu hệ thống phát hiện tấn công; các nguyên lý, phương pháp cũng như mô hình, kỹ thuật mã hóa; phân tích rủi ro và lập kế hoạch phục hồi hệ thống khi có sự cố.

- 11. Mục tiêu và chuẩn đầu ra của môn học**

11.1. Mục tiêu của môn học (COx)

Ký hiệu mục tiêu (COx)	Mô tả mục tiêu	Nội dung CĐR CTĐT phân bổ cho môn học	Ký hiệu CĐR CTĐT (PLOn)
(a)	(b)	(d)	(e)
CO1	Hiểu tổng quan về an toàn bảo mật, các thành phần, nguyên tắc, cũng như các vấn đề về hacker, virus, thiên tai...	Có kiến thức cơ bản về khoa học tự nhiên, khoa học xã hội, chính trị và pháp luật để vận dụng vào những vấn đề cuộc sống và trong các hoạt động nghề nghiệp.	PLO1
CO2	Biết, hiểu và vận dụng hệ thống phát hiện tấn công; các nguyên lý, phương pháp cũng như mô hình, kỹ thuật mã hóa;	Có khả năng vận dụng thành thạo kiến thức nền tảng và chuyên sâu để giải quyết các vấn đề chuyên môn	PLO6
CO3	Nắm được quy trình phân tích rủi ro và lập kế hoạch phục hồi hệ thống khi có sự cố.	Có khả năng thích ứng với các xu hướng thay đổi trong lĩnh vực chuyên môn, nghề nghiệp.	PLO8

11.2. Chuẩn đầu ra của môn học (CĐR MH) và sự đóng góp vào chuẩn đầu ra của chương trình đào tạo (CĐR CTĐT)

Ký hiệu CĐR MH (CLOi)	Nội dung CĐR MH	Mức độ theo thang đo	Đáp ứng mục tiêu môn học (COx)	Ký hiệu CĐR CTĐT (PLOn)
(a)	(b)	(c)	(d)	(e)
CLO1	Hiểu các khái niệm tổng quan về an toàn bảo mật, các rủi ro tiềm tàng liên quan đến an toàn bảo mật thông tin, hiểu một vài cấu hình hạ tầng, và vận hành được các thiết bị cơ	3	CO1	PLO1

	bản			
CLO2	Vận dụng được các phương pháp nhận dạng, kiểm tra thông tin trong mạng; Hiểu tổng quan các mối đe dọa đối với hệ thống mạng; Biết và hiểu được các bảo mật vật lý kiểm soát truy cập.	4	CO2	PLO6
CLO3	Vận dụng được các phương pháp mã hóa; Biết được tính pháp lý máy tính, bảo vệ chứng cứ, thu thập chứng cứ;	4	CO3	PLO8

11.3. Ma trận tích hợp giữa CDR MH (CLOi), CDR CTĐT (PLOn) và Chỉ số đánh giá kết quả thực hiện (PIn.k):

	PLO1		PLO6		PLO8	
	PI1.1	PI1.2	PI6.1	PI6.2	PI8.1	PI8.2
CLO1	3	3				
CLO2			4	4		
CLO3					4	4

12. Phương pháp và hình thức dạy và học

12.1. Phương pháp dạy và học:

Nhằm giúp sinh viên đạt được các mục tiêu và chuẩn đầu ra của môn học, các chiến lược và phương pháp giảng dạy được áp dụng cụ thể như sau:

- Phương pháp Thuyết giảng (Lecture): Giảng viên trình bày tài liệu và giải đáp các thắc mắc của học viên.
- Phương pháp Bài giảng tương tác (Interactive lecture): Thuyết giảng trong đó có quãng thời gian nghỉ khoảng từ hai đến mười lăm phút để cho sinh viên thực hiện các hoạt động học tập (chẳng hạn như: trả lời các câu hỏi trắc nghiệm nhiều lựa chọn, giải quyết vấn đề, bài tập so khớp và điền vào chỗ trống trong tập ghi chú bài giảng, vấn đáp về một trường hợp điển hình nhỏ, bài tập chia sẻ suy nghĩ theo cặp hoặc thảo luận nhóm nhỏ) cứ sau 12 đến 20 phút.

- Phương pháp Ôn luyện (Recitation): Học sinh trả lời các câu hỏi về kiến thức và đọc hiểu.
- Phương pháp Thảo luận có định hướng (Directed discussion): Thảo luận trong lớp theo một bộ câu hỏi ít nhiều có tính trật tự mà giảng viên đặt ra để dẫn dắt học sinh đến những nhận thức hoặc kết luận nhất định hoặc để giúp họ đạt được một kết quả học tập cụ thể.
- Phương pháp giảng dạy thông qua Làm việc/học tập theo nhóm (Group work/learning): người học thực hiện hoạt động học tập hoặc tạo ra một sản phẩm theo nhóm nhỏ từ hai đến sáu người trong hoặc ngoài lớp học, dưới sự hướng dẫn cẩn thận của giảng viên.

12.2. Hình thức dạy và học:

Giảng viên có thể chủ động lựa chọn hình thức giảng dạy là giảng dạy trực tiếp cho toàn bộ thời gian của môn học hoặc lựa chọn hình thức giảng dạy trực tuyến kết hợp trực tiếp, nhưng phải đảm bảo tổng thời gian giảng dạy trực tuyến không vượt quá 30% thời gian giảng dạy của cả môn học.

13. Quy định của môn học

- Sinh viên tuân thủ nghiêm túc các nội quy và quy định của Khoa và Trường.
- Đọc và nghiên cứu các tài liệu bài giảng trước khi lên lớp.
- Chấp hành nghiêm túc nội quy phòng máy.
- Thực hiện đầy đủ các bài tập thực hành được giao.
- Tham dự đầy đủ các buổi học trên lớp và các buổi thực hành do giảng viên trực tiếp hướng dẫn.
- Tự tìm hiểu thêm thông tin trên mạng Internet về các kiến thức liên quan đến môn học.
- Tham gia đầy đủ và tích cực các hoạt động trong quá trình học tập.
- Đối với bất kỳ sự gian lận nào trong quá trình làm bài tập hay bài thi, sinh viên phải chịu mọi hình thức kỷ luật theo quy định của Trường và bị 0 điểm cho nội dung đó.

14. Tài liệu học tập

14.1. Tài liệu bắt buộc

[1] Joel Scambray, Stuart McClure, George Kurtz, (2012). Hacking Exposed: Network Security Secrets & Solutions 7th, McGraw Hill.

14.2. Tài liệu tham khảo

[2] Kim, D., & Solomon, M. G., (2016). Fundamentals of information systems security: Print bundle. Jones & Bartlett Learning.

[3] Chapple, Mike, (2021). (ISC)² CISSP certified information systems security professional: official study guide, Ninth edition. - Hoboken : Sybex.

B. PHƯƠNG THỨC ĐÁNH GIÁ MÔN HỌC

1. Cơ cấu phương thức đánh giá môn học ¹

Loại hình đánh giá	Phương pháp đánh giá	Số lượng bài đánh giá	CĐR MH được đánh giá ²	Trọng số
1. Đánh giá quá trình	1.1. Đánh giá tính chuyên cần	2		10%
	1.2. Đánh giá quá trình 1	1	CLO1, CLO2	20%
	1.3. Đánh giá quá trình 2	1	CLO1, CLO2, CLO3	20%
2. Đánh giá cuối kỳ	2.1. Bài đánh giá cuối kỳ	1	CLO2, CLO3	50%

2. Phương pháp và công cụ đánh giá ³

2.1. Đánh giá quá trình

2.1.1. Đánh giá tính chuyên cần

- Đánh giá 1:

- Hình thức đánh giá: *điểm danh*.
- Thời điểm, cách thức thực hiện bài đánh giá: *ngẫu nhiên trong các buổi học*.
- Tỷ trọng: *70%*
- Nội dung, kết cấu bài đánh giá: *đánh giá sự hiện diện của sinh viên*.
- Rubric đánh giá:

¹ Khoa/Bộ môn phụ trách học phần cần thống nhất quy định về số lượng bài đánh giá trong mỗi phương thức đánh giá. Ví dụ: **1.2. Đánh giá quá trình 1 : 02 bài**.

² Mỗi bài đánh giá chỉ nên đáp ứng cho một CĐR môn học (ngoại trừ bài đánh giá cuối kỳ); rubric của mỗi bài đánh giá đều phải thể hiện (các) CĐR môn học mà bài đánh giá đó đảm nhận.

³ Xây dựng rubric đánh giá đi kèm theo từng bài đánh giá (tham khảo hướng dẫn xây dựng rubric đính kèm)

Tiêu chí đánh giá	Thang điểm			
	Dưới 5	5 – dưới 7	7 – dưới 9	9 - 10
Mức độ tham dự theo TKB	Số buổi vắng 4 buổi	Vắng 3 buổi	Vắng 1, 2 buổi	Không vắng buổi học nào

- Đánh giá 2:

- a. Hình thức đánh giá: *Ghi nhận quá trình tham gia học tập.*
- b. Thời điểm, cách thức thực hiện bài đánh giá:
 - Thời điểm: *tất cả các buổi học của học phần.*
 - Cách thức: *(1) giảng viên mời đích danh sinh viên trả lời các câu hỏi hay phân công giải quyết các bài tập/chủ đề thảo luận (tham gia thụ động), (2) sinh viên tự giác (xung phong) trả lời các câu hỏi hay tham gia giải quyết các bài tập/chủ đề thảo luận (tham gia chủ động)*
- c. Nội dung, kết cấu bài đánh giá: *mức độ tham gia vào quá trình học tập tại giảng đường.*
- d. Tỷ trọng: *30%*
- e. Rubric đánh giá:

Tiêu chí đánh giá	Thang điểm			
	Dưới 5	5 – dưới 7	7 – dưới 9	9 - 10
Mức độ tham gia các hoạt động học tập	Không bao giờ phát biểu trong giờ học	Có 1 lần phát biểu đúng hoặc giải bài tập tại lớp	Có 2, 3 lần phát biểu đúng hoặc giải bài tập đúng tại lớp	Có từ 4 lần trở lên phát biểu đúng hoặc giải bài tập đúng tại lớp

2.1.2. Đánh giá quá trình 1

- a. Hình thức đánh giá: *Bài kiểm tra cá nhân – trắc nghiệm*
- b. Thời điểm, cách thức thực hiện bài đánh giá:
 - Thời điểm: *sau khi học xong chương 05*
 - Cách thức: *kiểm tra tại lớp*
- c. Nội dung, kết cấu bài đánh giá: *20 câu trắc nghiệm, mỗi câu 0.5 điểm*
- d. Rubric đánh giá/hoặc Ma trận đề:

Tên chủ đề kiến thức	Các mức độ nhận thức			Tổng cộng	CLO
	Mức 2 (hiểu)	Mức 3	Mức 4		

		(vận dụng)	(phân tích)		
Chương 01. Các khái niệm tổng quan về bảo mật	Số câu: 4 Số điểm: 2.0 Tỉ lệ: 20%			Số câu: 4 Số điểm: 2.0 Tỉ lệ: 20%	CLO1
Chương 02. Các rủi ro tiềm tàng	Số câu: 2 Số điểm: 1 Tỉ lệ: 10%	Số câu: 2 Số điểm: 1 Tỉ lệ: 10%		Số câu: 4 Số điểm: 2.0 Tỉ lệ: 20%	CLO1
Chương 3. Hạ tầng và kết nối	Số câu: 4 Số điểm: 1 Tỉ lệ: 20%			Số câu: 4 Số điểm: 2.0 Tỉ lệ: 20 %	CLO1
Chương 4. Kiểm tra các hoạt động giao tiếp	Số câu: 2 Số điểm: 1 Tỉ lệ: 10%	Số câu: 2 Số điểm: 1 Tỉ lệ: 10%		Số câu: 4 Số điểm: 2.0 Tỉ lệ: 20 %	CLO2
Chương 5. Hiện thực và bảo trì mạng an toàn	Số câu: 2 Số điểm: 1 Tỉ lệ: 10 %	Số câu: 2 Số điểm: 1 Tỉ lệ: 10%		Số câu: 4 Số điểm: 2.0 Tỉ lệ: 20 %	CLO2
Tổng	Số câu: 14 Số điểm: 7 Tỉ lệ: 70%	Số câu: 6 Số điểm: 3 Tỉ lệ: 30%		Số câu: 20 Số điểm: 10 Tỉ lệ: 100%	

2.1.3. Đánh giá quá trình 2

- a. Hình thức đánh giá: bài tập lớn
- b. Thời điểm, cách thức thực hiện bài đánh giá:
 - o Thời điểm: tuần 01-03
 - o Cách thức: Giảng viên chia sinh viên thành các nhóm.
- c. Nội dung, kết cấu bài đánh giá:

Câu hỏi	Nội dung	Mức độ	CLO	Điểm (10đ)
1	Giới thiệu vấn đề	Hiểu	CLO1	2
2	Cơ sở lý luận (nền tảng/lý thuyết khoa học)	Hiểu	CLO2	3
3	Tổ chức lập luận để giải quyết vấn đề	Phân tích	CLO3	3
4	Trình bày báo cáo (thuyết trình + trả lời câu hỏi)	Vận dụng	CLO1 CLO2 CLO3	3

- d. Rubric đánh giá/hoặc Ma trận đề:

Tiêu chí đánh giá	CĐR	Trọng số	Thang điểm				
			Từ 0 đến 3,9	Từ 4,0 đến 5,4	Từ 5,5 đến 6,9	Từ 7,0 đến 8,4	Từ 8,5 đến 10
Cấu trúc của tiểu luận	CLO1	10%	Tiểu luận thiếu một trong hai phần: phần cơ sở lý luận khoa học liên quan; danh sách tác giả	Tiểu luận thiếu phần kết luận	Tiểu luận thiếu phần danh mục tài liệu tham khảo, danh mục bảng - hình	Tiểu luận thiếu mục lục tự động	Tiểu luận có đủ tất cả các phần theo quy định
Giới thiệu vấn đề	CLO1	10%	Không trình bày được tính cấp thiết (tầm quan trọng) của vấn đề	Trình bày không đúng về tính cấp thiết (tầm quan trọng) của vấn đề	Trình bày được nhưng chưa đủ về tính cấp thiết (tầm quan trọng) của vấn đề	Trình bày được về tính cấp thiết (tầm quan trọng) của vấn đề nhưng chưa thuyết phục người đọc	Phân tích rõ ràng, rất thuyết phục về tính cấp thiết (tầm quan trọng) của vấn đề
Cơ sở lý luận (nền tảng/lý thuyết khoa học)	CLO2	20%	Không sử dụng lý luận khoa học liên	Có sử dụng nhưng chưa đúng lý	Trình bày lý luận khoa học liên	Sử dụng đúng lý luận khoa học liên	Sử dụng chính xác, rất thuyết phục về

Tiêu chí đánh giá	CĐR	Trọng số	Thang điểm				
			Từ 0 đến 3,9	Từ 4,0 đến 5,4	Từ 5,5 đến 6,9	Từ 7,0 đến 8,4	Từ 8,5 đến 10
			quan	luận khoa học liên quan	quan, nhưng chưa đủ sức thuyết phục	quan, có sức thuyết phục	lý luận khoa học liên quan
Tổ chức lập luận để giải quyết vấn đề	CLO3	20%	Không có logic trong lập luận; thiếu minh chứng	Lập luận còn lỏng lẻo; minh chứng thiếu tính thuyết phục	Lập luận và minh chứng có thể chấp nhận được	Lập luận tương đối chặt chẽ; minh chứng thuyết phục	Lập luận chặt chẽ; minh chứng thuyết phục
Văn phong khoa học	CLO1	10%	Hành văn tối nghĩa ở các phần nội dung chính	Hành văn lung củng khiến cho người đọc khó có thể hiểu nội dung	Hành văn lung củng nhưng người đọc vẫn có thể hiểu nội dung	Hành văn tốt, đôi khi có lỗi diễn đạt	Hành văn rõ ràng, mạch lạc
Lỗi đạo văn			Theo quy định của CTĐT				
Hình thức	CLO1	10%	Không định dạng theo bất cứ tiêu chí nào	Có lỗi: không căn lề, không thống nhất định dạng đoạn văn, sai	Có lỗi: Không định dạng toàn văn bản, không thống nhất font	Có lỗi: thiếu đánh số trang; thiếu bìa hoặc trình bày bìa sai quy định	Định dạng đúng tất cả các tiêu chí yêu cầu

Tiêu chí đánh giá	CĐR	Trọng số	Thang điểm				
			Từ 0 đến 3,9	Từ 4,0 đến 5,4	Từ 5,5 đến 6,9	Từ 7,0 đến 8,4	Từ 8,5 đến 10
				khở giấy	chữ		
Báo cáo bài nhóm (chỉ chấm cho nhóm đạt tiêu chuẩn để báo cáo)							
+ Thuyết trình báo cáo	CLO1	10%	Không thể báo cáo được bài tiểu luận	Báo cáo bài kém thuyết phục; tương tác chưa tốt; quản lý thời gian chưa tốt	Báo cáo bài lỗi cuốn, thuyết phục; tương tác chưa tốt; quản lý thời gian chưa tốt	Báo cáo bài lỗi cuốn, thuyết phục; tương tác tốt; quản lý thời gian chưa tốt	Báo cáo bài lỗi cuốn, thuyết phục; tương tác tốt; quản lý thời gian tốt
+ Trả lời câu hỏi	CLO2	10%	Không trả lời được các câu hỏi đặt hỏi đúng	Trả lời đầy đủ, rõ ràng, và thỏa đáng cho chỉ dưới 1/2 các câu hỏi đặt hỏi đúng	Trả lời đầy đủ, rõ ràng, và thỏa đáng từ 1/2 các câu hỏi đặt hỏi đúng trở lên; các câu còn lại chưa có hướng trả lời	Trả lời đầy đủ, rõ ràng, và thỏa đáng từ 1/2 các câu hỏi đặt hỏi đúng trở lên; các câu còn lại có hướng trả lời chấp nhận được	Trả lời đầy đủ, rõ ràng, và thỏa đáng cho tất cả các câu hỏi đặt hỏi đúng

2.2. Đánh giá cuối kỳ

- Đề thi do Khoa/Bộ môn quản lý học phân ra đề hoặc trích xuất từ Ngân hàng câu hỏi thi/Ngân hàng đề thi của Trường (nếu có).

- Hình thức đánh giá: (đánh dấu X lựa chọn hình thức đánh giá)

Hình thức đánh giá		Lựa chọn
Vấn đáp		
Tự luận		
Trắc nghiệm khách quan		X
Trắc nghiệm khách quan kết hợp tự luận		
Thực hành trên máy tính		
Tiểu luận/đồ án/bài tập lớn (cá nhân)	Nộp bài không thuyết trình	
	Nộp bài có thuyết trình	
Tiểu luận/đồ án/bài tập lớn (nhóm)	Nộp bài không thuyết trình	
	Nộp bài có thuyết trình	

- Thời gian làm bài (tối thiểu – tối đa): 60 phút - 75 phút
- Mô tả về kết cấu đề thi: 40 câu hỏi trắc nghiệm.
- Mô tả về phạm vi nội dung của đề thi: các chương 1 đến 9
- Rubric đánh giá/hoặc Ma trận đề:

Tên chủ đề kiến thức	Các mức độ nhận thức			Tổng cộng	CLO
	Mức 2 (hiểu)	Mức 3 (vận dụng)	Mức 4 (phân tích)		
Các khái niệm tổng quan về bảo mật	Số câu: 4 Số điểm: 1.0 Tỉ lệ: 10 %			Số câu: 4 Số điểm: 1.0 Tỉ lệ: 10 %	CLO1
Các rủi ro tiềm tàng	Số câu: 2 Số điểm: 0.5 Tỉ lệ: 5%	Số câu: 2 Số điểm: 0.5 Tỉ lệ: 5%	Số câu: 2 Số điểm: 0.5 Tỉ lệ: 5%	Số câu: 6 Số điểm: 1.5 Tỉ lệ: 15%	CLO1
Hạ tầng và kết nối	Số câu: 4 Số điểm: 1 Tỉ lệ: 10%			Số câu: 4 Số điểm: 1.0 Tỉ lệ: 10 %	CLO2
Kiểm tra các hoạt động giao tiếp		Số câu: 4 Số điểm: 1		Số câu: 4 Số điểm:	CLO2

		Tỉ lệ: 10%		1.0 Tỉ lệ: 10 %	
Hiện thực và bảo trì mạng an toàn	Số câu: 4 Số điểm: 1.0 Tỉ lệ: 10 %			Số câu: 4 Số điểm: 1.0 Tỉ lệ: 10 %	CLO2
Bảo mật mạng và môi trường	Số câu: 2 Số điểm: 0.5 Tỉ lệ: 5%	Số câu: 2 Số điểm: 0.5 Tỉ lệ: 5%		Số câu: 4 Số điểm: 1.0 Tỉ lệ: 10%	CLO2
Mật mã, các phương pháp, và các chuẩn mã hóa		Số câu: 4 Số điểm: 0.5 Tỉ lệ: 10%	Số câu: 2 Số điểm: 0.5 Tỉ lệ: 5%	Số câu: 6 Số điểm: 1.5 Tỉ lệ: 15 %	CLO3
Các chính sách và thủ tục bảo mật	Số câu: 4 Số điểm: 1.0 Tỉ lệ: 10 %			Số câu: 4 Số điểm: 1.0 Tỉ lệ: 10 %	CLO1
Quản trị bảo mật		Số câu: 4 Số điểm: 1.0 Tỉ lệ: 10 %		Số câu: 4 Số điểm: 1.0 Tỉ lệ: 10 %	CLO3
Tổng số câu: Tổng số điểm: Tỉ lệ:	20 5.0 50%	16 4 40%	4 1 10%	40 10 100%	

- Quy định về việc sử dụng tài liệu: *được sử dụng tài liệu.*
- Các quy định khác về bài đánh giá: *không.*

C. NỘI DUNG CHI TIẾT GIẢNG DẠY

Thời lượng (giờ)	Nội dung giảng dạy	CDR MH	Hoạt động Phương pháp dạy và học	Bài đánh giá	Học liệu
(a)	(b)	(c)	(d)	(e)	(f)
3	<p>CHƯƠNG 1: CÁC KHÁI NIỆM TỔNG QUAN VỀ BẢO MẬT</p> <p>1.1 Bảo mật thông tin</p> <p>1.1.1 Các khái niệm</p> <p>1.1.2 Bảo mật vật lý</p> <p>1.1.3 Bảo mật hoạt động</p> <p>1.1.4 Quản lý và các chính sách</p> <p>1.2 Mục đích của bảo mật thông tin</p> <p>1.3 Quá trình bảo mật</p> <p>1.3.1 Triển khai phần mềm chống virus</p> <p>1.3.2 Hiện thực kiểm soát truy cập</p> <p>1.3.3 Chứng thực</p> <p>1.3.4 Các dịch vụ và các giao thức mạng</p> <p>1.4 Phân biệt các mô hình bảo mật</p> <p>1.4.1 Mục đích thiết kế</p> <p>1.4.2 Các vùng bảo mật</p> <p>1.4.3 Các kỹ thuật</p> <p>1.4.4 Các yêu cầu của doanh nghiệp</p>	CLO1	<p>GIẢNG VIÊN:</p> <p>Giới thiệu môn học (chú ý: giáo trình, công bố lịch bài tập về nhà, giao đề tài bài tiểu luận nhóm).</p> <p>Giảng bài, vấn đáp về các khái niệm cơ bản.</p> <p>Giao sinh viên chuẩn bị bài Chương 2.</p> <p>Giao bài tập về nhà</p> <p>SINH VIÊN:</p> <p>Nghe giảng, tham gia thảo luận, phát biểu ý kiến xây dựng bài.</p> <p>Trả lời câu hỏi của giảng viên.</p>	1.1 1.2 1.3 2.1	[2]
7	<p>CHƯƠNG 2: CÁC RỦI RO TIỀM TÀNG</p> <p>2.1 Tính toán các chiến thuật tấn công</p> <p>2.1.1 Tấn công truy xuất</p>	CLO2	<p>Giảng viên:</p> <p>- Trình bày các rủi ro tiềm tàng.</p>	1.1 1.2	[2] và [3]

Thời lượng (giờ)	Nội dung giảng dạy	CĐR MH	Hoạt động Phương pháp dạy và học	Bài đánh giá	Học liệu
(a)	(b)	(c)	(d)	(e)	(f)
	2.1.2 Tấn công phản đối, chỉnh sửa 2.1.3 Tấn công từ chối dịch vụ (DoS) 2.2 Các tấn công phổ biến 2.2.1 Back-door 2.2.2 Spoofing 2.2.3 Man in the middle 2.2.4 Replay 2.2.5 Đoán mật khẩu 2.3 Những vấn đề về bảo mật TCP/IP 2.3.1 Làm việc với các giao thức 2.3.2 Xác định các tấn công TCP/IP 2.4 Các chương trình nguy hại 2.4.1 Virus 2.4.2 Trojan 2.4.3 Logic bomb 2.4.4 Worm 2.4.5 Ransomware 2.4.6 Vấn đề con người		- Giới thiệu bài thực hành 1, 2 nhằm tìm hiểu về các chương trình diệt virus thông dụng, đĩa công cụ Hiren, phần mềm OphCrack. Sinh viên: - Lắng nghe, biết và hiểu nội dung bài. - Thực hành bài thực hành số 1, 2.	1.3 2.1	
6	CHƯƠNG 3: HẠ TẦNG VÀ KẾT NỐI 3.1 Bảo mật cơ sở hạ tầng 3.1.1 Các thành phần phần cứng 3.1.2 Các thành phần phần mềm	CLO3	Giảng viên: - Trình bày nội dung - Đưa ra tình huống cụ thể mô hình mạng được triển khai	1.1 1.2	[3]

Thời lượng (giờ)	Nội dung giảng dạy	CDR MH	Hoạt động Phương pháp dạy và học	Bài đánh giá	Học liệu
(a)	(b)	(c)	(d)	(e)	(f)
	3.2 Sự khác biệt của các thiết bị mạng nền tảng 3.2.1 Tường lửa 3.2.2 Hub 3.2.3 Bộ định tuyến (Router) 3.2.4 Bộ chuyển mạch (Switch) 3.2.5 Điểm truy cập không dây (Wireless Access Point) 3.2.6 Các dịch vụ truy cập từ xa (RAS) 3.2.7 Hệ thống Telecoms/PBX 3.2.8 Các mạng riêng ảo (VPN)		trong phòng máy. Qua đó giới thiệu bài tập số 3 Sinh viên: - lắng nghe, biết và hiểu. Thực hành bài thực hành 3	1.3 2.1	
9	CHƯƠNG 4: KIỂM TRA CÁC HOẠT ĐỘNG GIAO TIẾP 4.1 Kiểm tra mạng 4.1.1 Nhận dạng các luồng thông tin mạng 4.1.2 Quản lý các hệ thống mạng 4.2 Các hệ thống phát hiện xâm nhập 4.2.1 Network-Based IDS 4.2.2 Host-Based IDS 4.2.3 Honey Pot 4.2.4 Đáp ứng rắc rối 4.3 Các hệ thống không dây 4.3.1 Lớp vận chuyển không dây an toàn	CLO3	Giảng viên: - Trình bày các nội dung của chương, giới thiệu các phần mềm gửi nhận thông điệp - Giới thiệu thêm về các công cụ phát hiện gói, phân tích tín hiệu Sinh viên: - Lắng nghe, biết và hiểu nội dung bài. - Thực hành bài thực hành 4	1.1 1.2 1.3 2.1	[2] và [3]

Thời lượng (giờ)	Nội dung giảng dạy	CĐR MH	Hoạt động Phương pháp dạy và học	Bài đánh giá	Học liệu
(a)	(b)	(c)	(d)	(e)	(f)
	4.3.2 Các giao thức không dây IEEE 802.11x 4.3.3 WEP/WAP 4.4 Các đặc điểm của các phần mềm gửi nhận thông điệp 4.5 Phát hiện gói 4.6 Phân tích tín hiệu 4.6.1 Foot-printing 4.6.2 Scanning				
7	CHƯƠNG 5: HIỆN THỰC VÀ BẢO TRÌ MẠNG AN TOÀN 5.1 Tổng quan về các mối đe dọa của mạng 5.2 Nền tảng bảo mật 5.3 Củng cố OS và NOS 5.4 Củng cố các thiết bị mạng 5.4.1 Cập nhật phần mềm điều khiển thiết bị 5.4.2 Cài đặt cấu hình bộ định tuyến/bộ chuyển mạch 5.5 Củng cố các ứng dụng 5.5.1 Dịch vụ web 5.5.2 Dịch vụ email 5.5.3 Dịch vụ truyền nhận tập tin 5.5.4 Dịch vụ tên miền	CLO2 , CLO3	Giảng viên: - Trình bày các nội dung của chương Sinh viên: - Lắng nghe, biết và hiểu nội dung bài, đặt câu hỏi cho những nội dung chưa hiểu và hướng phát triển. - Thực hành cập nhật củng cố phần mềm điều khiển thiết bị, củng cố các ứng dụng. Thực hành bài thực hành số 5	1.1 1.2 1.3 2.1	[3]

Thời lượng (giờ)	Nội dung giảng dạy	CDR MH	Hoạt động Phương pháp dạy và học	Bài đánh giá	Học liệu
(a)	(b)	(c)	(d)	(e)	(f)
	5.5.5 Các dịch vụ chia sẻ tập tin và máy in 5.5.6 Dịch vụ DHCP				
3	CHƯƠNG 6: BẢO MẬT MẠNG VÀ MÔI TRƯỜNG 6.1 Bảo mật vật lý và mạng 6.1.1 Hiện thực kiểm soát truy cập 6.1.2 Tìm hiểu tâm lý người dùng 6.1.3 Quét môi trường 6.2 Kế hoạch kinh doanh 6.2.1 Phân tích tác động an toàn trong việc kinh doanh 6.2.2 Đánh giá rủi ro 6.3 Phát triển các chính sách, các chuẩn và các hướng dẫn 6.3.1 Hiện thực các chính sách 6.3.2 Các chuẩn kết hợp 6.3.3 Một số hướng dẫn 6.4 Phân loại thông tin 6.4.1 Thông tin chung 6.4.2 Thông tin cá nhân 6.4.3 Vai trò trong quy trình an toàn 6.4.4 Kiểm soát truy cập thông tin	CLO2 , CLO3	Giảng viên: trình bày các nội dung của chương Sinh viên: lắng nghe, biết và hiểu nội dung bài	1.1 1.2 2.1	[2]

Thời lượng (giờ)	Nội dung giảng dạy	CĐR MH	Hoạt động Phương pháp dạy và học	Bài đánh giá	Học liệu
(a)	(b)	(c)	(d)	(e)	(f)
6	<p>CHƯƠNG 7: MẬT MÃ, CÁC PHƯƠNG PHÁP, VÀ CÁC CHUẨN MÃ HÓA</p> <p>7.1 Tổng quan về mật mã</p> <p>7.1.1 Tìm hiểu mã hóa vật lý</p> <p>7.1.2 Tìm hiểu mã hóa toán học</p> <p>7.1.3 Tìm hiểu mã hóa lượng tử</p> <p>7.2 Các thuật giải mã hóa</p> <p>7.2.1 Hashing</p> <p>7.2.2 Các thuật giải mã hóa đối xứng</p> <p>7.2.3 Các thuật giải mã hóa bất đối xứng</p> <p>7.3 Các vấn đề sử dụng hệ thống mã hóa</p> <p>7.3.1 Bảo mật</p> <p>7.3.2 Nhất quán</p> <p>7.3.3 Xác thực</p> <p>7.3.4 Không thoái thác</p> <p>7.3.5 Kiểm soát truy cập</p> <p>7.4 Kiến trúc hạ tầng khóa công cộng</p> <p>7.4.1 Sử dụng chứng thực quyền</p> <p>7.4.2 Hiện thực các chứng chỉ</p> <p>7.4.3 Thu hồi các chứng chỉ</p> <p>7.4.4 Hiện thực các mô hình tin cậy</p> <p>7.5 Đối phó với các tấn công mã hóa</p>	<p>CLO1</p> <p>,</p> <p>CLO2</p> <p>,</p> <p>CLO3</p>	<p>Giảng viên: trình bày các nội dung của chương</p> <p>Sinh viên: lắng nghe, biết và hiểu nội dung bài</p>	<p>1.1</p> <p>1.3</p> <p>2.1</p>	[2] và [3]

Thời lượng (giờ)	Nội dung giảng dạy	CĐR MH	Hoạt động Phương pháp dạy và học	Bài đánh giá	Học liệu
(a)	(b)	(c)	(d)	(e)	(f)
	<p>7.6 Các chuẩn và các giao thức mã hóa</p> <p>7.6.1 Các chuẩn mã hóa cổ điển</p> <p>7.6.2 X.509</p> <p>7.6.3 SSL và TLS</p> <p>7.6.4 SSH</p> <p>7.6.5 HTTPS</p> <p>7.7 Quản trị khóa và chu kỳ thời gian của khóa</p> <p>7.7.1 So sánh khóa tập trung và khóa không tập trung</p> <p>7.7.2 Lưu trữ và phân phối khóa</p> <p>7.7.3 Sử dụng mô hình ký quỹ khóa</p> <p>7.7.4 Hạn sử dụng khóa</p> <p>7.7.5 Thu hồi khóa</p> <p>7.7.6 Tạm hoãn khóa</p> <p>7.7.7 Phục hồi và lưu giữ khóa</p> <p>7.7.8 Cấp mới khóa</p> <p>7.7.9 Hủy khóa</p>				
2	<p>CHƯƠNG 8: CÁC CHÍNH SÁCH VÀ THỦ TỤC BẢO MẬT</p> <p>8.1 Tính liên tục của kinh doanh</p> <p>8.1.1 Lợi ích</p> <p>8.1.2 Tính sẵn có cao</p>	<p>CLO1</p> <p>,</p> <p>CLO2</p> <p>,</p> <p>CLO3</p>	<p>GIẢNG VIÊN:</p> <p>Giảng bài mới.</p> <p>Điểm danh</p> <p>Hướng dẫn làm bài tập lớn</p> <p>SINH VIÊN:</p>	<p>1.1</p> <p>1.3</p> <p>2.1</p>	[3]

Thời lượng (giờ)	Nội dung giảng dạy	CĐR MH	Hoạt động Phương pháp dạy và học	Bài đánh giá	Học liệu
(a)	(b)	(c)	(d)	(e)	(f)
	8.1.3 Phục hồi sự cố 8.2 Củng cố hỗ trợ các nhà cung cấp 8.2.1 Các bản thỏa thuận dịch vụ 8.2.2 Ký quỹ mã nguồn 8.3 Tạo các chính sách và thủ tục 8.3.1 Chính sách nguồn nhân lực 8.3.2 Chính sách kinh doanh 8.3.3 Chính sách chứng chỉ 8.3.4 Chính sách đáp ứng rắc rối 8.4 Củng cố quản trị quyền 8.4.1 Vai trò quản trị user và nhóm 8.4.2 Quyền tăng cường 8.4.3 Quyền ra quyết định		Nghe giảng, tham gia thảo luận, phát biểu ý kiến xây dựng bài. - Hội giảng viên các vấn đề về bài tập lớn và hoàn thành		
2	CHƯƠNG 9: QUẢN TRỊ BẢO MẬT 9.1 Các pháp lý về máy tính 9.1.1 Phương pháp luận của điều tra pháp lý 9.1.2 Thi hành chuỗi liên đới 9.1.3 Bảo vệ chứng cứ 9.1.4 Thu thập chứng cứ 9.2 Quản trị bảo mật 9.3 Kiến thức và giáo dục bảo mật 9.3.1 Sử dụng truyền thông và nâng cao nhận thức	CLO1 , CLO2 , CLO3	GIẢNG VIÊN: Giảng bài. Thông báo điểm quá trình Thu tập lớn SINH VIÊN: Nghe giảng, tham gia thảo luận, phát biểu ý kiến xây dựng bài. -Xem điểm, đề nghị điều chỉnh sai sót (nếu có) và xác nhận điểm.	1.1 1.3 2.1	[3]

Thời lượng (giờ)	Nội dung giảng dạy	CĐR MH	Hoạt động Phương pháp dạy và học	Bài đánh giá	Học liệu
(a)	(b)	(c)	(d)	(e)	(f)
	9.3.2 Giáo dục 9.3.3 Điều lệ bí mật cá nhân và bảo mật		- Trao đổi với giảng viên, cả lớp về các nội dung đã học		

TRƯỞNG BỘ MÔN



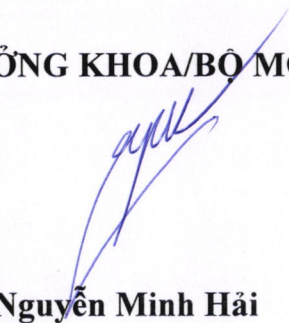
Nguyễn Minh Hải

NGƯỜI BIÊN SOẠN



Nguyễn Thanh Hiền

TRƯỞNG KHOA/BỘ MÔN



Nguyễn Minh Hải

HIỆU TRƯỞNG



Nguyễn Đức Trung