BỘ CÔNG THƯƠNG
TRƯỜNG ĐẠI HỌC SAO ĐỎ
*****

ĐỀ CƯƠNG CHI TIẾT HỌC PHẦN
AN TOÀN VÀ AN NINH MẠNG

Số tín chỉ: 3 (2, 1)
Trình độ đào tạo: Đại học
Ngành: Công nghệ thông tin

Năm 2020

TRƯỜNG ĐẠI HỌC SAO ĐỎ
KHOA: ĐIỆN TỬ - TIN HỌC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

ĐỀ CƯƠNG CHI TIẾT HỌC PHẦN
Trình độ đào tạo: Đại học
Ngành: Công nghệ thông tin

1. Tên học phần: An toàn và an ninh mạng
2. Mã học phần: CNTT 201
3. Số tín chỉ: 3 (2, 1)
4. Trình độ cho sinh viên: Năm thứ tư
5. Phân bổ thời gian
- Lên lớp: 30 tiết lý thuyết, 30 tiết thực hành
- Tự học: 90 giờ

6. Điều kiện tiên quyết
7. Giảng viên

STT	Học hàm, học vị, họ tên	Số điện thoại	Email
1	ThS. Nguyễn Phúc Hậu	0929130000	phuchauptit@gmail.com
2	ThS. Vũ Bảo Tạo	0384305659	taovb2006@gmail.com
3	ThS. Nguyễn Thị Ánh Tuyết	0972384233	anhtuyet13381@gmail.com

8. Mô tả nội dung của học phần

Học phần An toàn và an ninh mạng gồm các nội dung khái lược về an toàn và thông tin dữ liệu, những nội dung cơ bản trong an ninh mạng; lỗ hổng bảo mật và các loại tấn công phổ biến; an ninh mạng mức giao vận; an ninh thư điện tử; an toàn và an ninh mạng máy tính; một số kỹ thuật phát hiện xâm nhập và phòng thủ trong an ninh mạng. Thông qua học phần giúp sinh viên ghi nhớ, phân loại, thực hiện cũng như đánh giá mức độ an toàn của hệ thống mạng.

9. Mục tiêu và chuẩn đầu ra học phần

9.1. Mục tiêu

Mục tiêu học phần thỏa mãn mục tiêu của chương trình đào tạo:

Mục tiêu	Mô tả	Mức độ theo thang đo Bloom	Phân bổ mục tiêu học phần trong CTĐT
MT1	**Kiến thức**		
MT1.1	Trình bày được tầm quan trọng an toàn và an ninh mạng trong vấn đề quản lý dữ liệu, an toàn khi truyền dữ liệu trong môi trường mạng máy tính.	2	[1.2.1.2a]

Mục tiêu	Mô tả	Mức độ theo thang đo Bloom	Phân bổ mục tiêu học phần trong CTĐT
MT1.2	Hiểu được các chiến lược an toàn hệ thống, các phương pháp an toàn mạng, một số lỗ hổng và cách thức tấn công mạng của hacker, một số kỹ thuật phát hiện xâm nhập và phòng thủ trong an ninh mạng.	2	
MT2	**Kỹ năng**		
MT2.1	Có kỹ năng phòng chống xâm nhập trong mạng máy tính, làm việc độc lập, làm việc nhóm, tư duy, áp dụng các kỹ thuật để phân tích phương án và triển khai phát hiện xâm nhập và phòng thủ trong an ninh mạng.	3	[1.2.2.1]
MT2.2	Có khả năng thích ứng với sự thay đổi của công nghệ mạng máy tính nói riêng và các công nghệ khác nói chung.	3	
MT3	**Mức tự chủ và trách nhiệm**		
MT3.1	Có năng lực định hướng, lập kế hoạch, điều phối, quản lý, hướng dẫn, giám sát, đánh giá và đưa ra kết luận các công việc thuộc chuyên môn nghề nghiệp.	4	[1.2.3.2]
MT3.2	Có thái độ tích cực trong học tập và chịu trách nhiệm với các nhiệm vụ được phân công.	4	

9.2. Chuẩn đầu ra

Sự phù hợp của chuẩn đầu ra học phần với chuẩn đầu ra của chương trình đào tạo:

CĐR học phần	Mô tả	Thang đo Bloom	Phân bổ CĐR học phần trong CTĐT
CĐR1	**Kiến thức**		
CĐR1.1	Trình bày và phân tích được sự an toàn và an ninh mạng trong việc quản lý dữ liệu, truyền dữ liệu trong	2	[2.1.6]

CĐR học phần	Mô tả	Thang đo Bloom	Phân bổ CĐR học phần trong CTĐT
	môi trường mạng máy tính.		
CĐR1.2	Phân biệt được các phương pháp an toàn mạng, một số lỗ hổng và cách thức tấn công mạng của hacker.	4	
CĐR1.3	Trình bày được một số kỹ thuật phát hiện xâm nhập và phòng thủ trong an ninh mạng.	2	
CĐR1.4	Tổ chức và kiểm tra an toàn và an ninh mạng trong các hệ thống mạng.	2	
CĐR2	**Kỹ năng**		
CĐR2.1	Kiểm tra và triển khai được phương án phòng chống xâm nhập trong mạng máy tính, làm việc độc lập, làm việc nhóm, tư duy, áp dụng các kỹ thuật để phát hiện xâm nhập và phòng thủ trong an ninh mạng.	3	[2.2.6]
CĐR2.2	Có khả năng tổ chức, triển khai hệ thống mạng máy tính nói chung.	3	
CĐR3	**Mức tự chủ và trách nhiệm**		
CĐR3.1	Có khả năng phân biệt, tổ chức với những nhiệm vụ được giao.	4	[2.3.1]
CĐR3.2	Có năng lực hướng dẫn, giám sát người khác cùng thực hiện nhiệm vụ chuyên môn.	4	[2.3.2]

10. Ma trận liên kết nội dung với chuẩn đầu ra học phần

Chương	Nội dung học phần	Chuẩn đầu ra của học phần							
		CĐR1				CĐR2		CĐR3	
		CĐR 1.1	CĐR 1.2	CĐR 1.3	CĐR 1.4	CĐR 2.1	CĐR 2.2	CĐR 3.1	CĐR 3.2
1	**Chương I. An toàn và thông tin dữ liệu** 1.1. Tổng quan an toàn thông tin dữ liệu 1.2. Đánh giá độ an toàn bảo vệ thông tin dữ liệu 1.3. Các chiến lược an toàn hệ thống 1.4. Các mức bảo vệ trên mạng 1.5. An toàn thông tin bằng mật mã 1.6. Vai trò của hệ mật mã 1.7. Các nguy cơ đe dọa	x			x				

Chương	Nội dung học phần	Chuẩn đầu ra của học phần							
		CĐR1				CĐR2		CĐR3	
		CĐR 1.1	CĐR 1.2	CĐR 1.3	CĐR 1.4	CĐR 2.1	CĐR 2.2	CĐR 3.1	CĐR 3.2
2	**Chương II. Các vấn đề trong an ninh mạng** 2.1. Mục tiêu của an ninh mạng 2.2. Tấn công mạng 2.3. Lỗ hổng bảo mật và các loại tấn công phổ biến 2.4. Các lĩnh vực trong tấn công mạng	x		x	x				
3	**Chương III. An ninh mức giao vận và thư điện tử** 3.1. Vấn đề an ninh Website 3.2. Giao thức Secure Sockets Layer 3.3. Chuẩn Transport Layer Security 3.4. Giao thức Secure Shell 3.5 Chương trình Pretty Good Privacy 3.6. Chuẩn Multipurpose Internet Mail Extensions 3.7. Giao thức Hypertext Transfer Protocol Secure 3.8. Giáo thức SSH	x	x	x	x				
4	**Chương IV. An ninh và an toàn mạng máy tính** **4.1. Khái niệm lỗ hổng** 4.2. Các lỗ hổng bảo mật của hệ điều hành 4.3. Các lỗ hổng bảo mật của mạng máy tính 4.4. Một số lỗ hổng do người dùng vô tình gây ra 4.5. Hackers và hậu quả hacker gây ra 4.6. Tấn công mạng qua lỗ hổng	x		x		x		x	
5	**Chương V. Một số kỹ thuật phát hiện xâm nhập và phòng thủ trong an ninh mạng** 5.1. Một số kỹ thuật phòng thủ 5.2. Hệ thống phát hiện xâm nhập IDS 5.3. Phát hiện dấu hiệu không bình thường 5.4. Các mẫu hành vi thông thường, phát hiện bất thường 5.5. Một số kỹ thuật xử lý dữ liệu sử dụng trong các hệ thống phát hiện xâm nhập	x	x	x		x		x	x

11. Đánh giá học phần

11.1. Kiểm tra và đánh giá trình độ

Chuẩn đầu ra	Mức độ thành thạo được đánh giá bởi
CĐR1	Kiểm tra thường xuyên, kiểm tra thực hiện nhiệm vụ về nhà, kiểm tra giữa học phần.
CĐR2	Kết quả thảo luận trên lớp, thực hiện nhiệm vụ về nhà, bài tiểu

	luận kiểm tra giữa học phần.
CĐR3	Kiểm tra thường xuyên, kết quả thực hiện nhiệm vụ của cá nhân và theo nhóm, bài báo cáo kết thúc học phần.

11.2. Cách tính điểm học phần: Tính theo thang điểm 10 sau đó chuyển thành thang điểm chữ và thang điểm 4.

STT	Điểm thành phần	Quy định	Trọng số	Ghi chú
1	Điểm thường xuyên, đánh giá nhận thức, thái độ thảo luận, chuyên cần của sinh viên.	01 điểm	20%	Điểm trung bình của các lần đánh giá
2	Kiểm tra giữa học phần	01 điểm	30%	
3	Thi kết thúc học phần	01 điểm	50%	

11.3. Phương pháp đánh giá

- Đánh giá thường xuyên, chuyên cần, thực hành: Vấn đáp, tỷ lệ hiện diện trên lớp, làm bài tập thực hành,…
- Kiểm tra giữa học phần: Báo cáo sơ bộ bài tập lớn 01 tiết.
- Thi kết thúc học phần: Báo cáo bài tập lớn 02 tiết.

12. Yêu cầu học phần

- Yêu cầu về thái độ học tập, chuyên cần: Hoàn thành bài tập và nhiệm vụ giảng viên giao, tham dự ít nhất 80% thời lượng học phần; ghi chép và tích cực thảo luận, xây dựng bài trên lớp.
- Yêu cầu về nghiên cứu tài liệu: Nghiên cứu tài liệu trước khi đến lớp, đọc thêm các tài liệu liên quan được giảng viên giới thiệu.
- Yêu cầu về kiểm tra giữa học phần và thi kết thúc học phần: Sinh viên thực hiện theo quy chế.

13. Tài liệu phục vụ học phần

- Tài liệu bắt buộc:

[1] - Trường Đại học Sao Đỏ (2020), *Giáo trình An toàn và an ninh mạng*.

- Tài liệu tham khảo:

[2] - Trường Đại học Sao Đỏ (2018), *Giáo trình Bảo mật thông tin*.

[3] - NXB Công thương (2018), *Bóng ma trên mạng.*

14. Nội dung chi tiết học phần và phương pháp dạy-học

TT	Nội dung giảng dạy	Số tiết	Phương pháp dạy-học	CĐR học phần
1.	**Chương I. An toàn và thông tin dữ liệu** **Mục tiêu chương:** Trình bày được vấn đề an toàn thông tin dữ liệu, đánh giá độ an toàn bảo vệ thông tin dữ liệu, các chiến lược an toàn hệ	8 (4LT, 4TH)	**Thuyết trình, đàm thoại nêu vấn đề** **- Giảng viên:** + Giảng giải, đàm thoại làm rõ các nội dung.	CĐR1.1 CĐR1.4

TT	Nội dung giảng dạy	Số tiết	Phương pháp dạy-học	CĐR học phần
	thống, các mức bảo vệ trên mạng, an toàn thông tin bằng mật mã, vai trò của hệ mật mã và các nguy cơ đe dọa trong vấn đề an ninh mạng. **Nội dung cụ thể:** 1.1. Tổng quan an toàn thông tin dữ liệu 1.2. Đánh giá độ an toàn bảo vệ thông tin dữ liệu 1.3. Các chiến lược an toàn hệ thống 1.4. Các mức bảo vệ trên mạng 1.5. An toàn thông tin bằng mật mã 1.6. Vai trò của hệ mật mã 1.7. Các nguy cơ đe dọa Bài thực hành chương 1		+ Giải quyết các vấn đề an ninh mạng trong thực tiễn. + Giao nội dung thực hành. + Nhận xét đánh giá **- Sinh viên:** + Đọc trước tài liệu [1] - chương 1 mục 1.1 - 1.7. + Lắng nghe, quan sát, ghi chép, trả lời câu hỏi. + Làm bài tập chương 1. + Đọc tài liệu tham khảo tài liệu [3] phần 1.	
2.	**Chương II. Các vấn đề trong an ninh mạng** **Mục tiêu chương:** Trình bày được mục tiêu của an ninh mạng, tấn công mạng, lỗ hổng bảo mật và các loại tấn công phổ biến, các lĩnh vực tấn công mạng. **Nội dung cụ thể:** 2.1. Mục tiêu của an ninh mạng 2.2. Tấn công mạng 2.3. Lỗ hổng bảo mật và các loại tấn công phổ biến 2.4. Các lĩnh vực trong tấn công mạng Bài thực hành chương 2	8 (4LT, 4TH)	**Thuyết trình, đàm thoại nêu vấn đề** **- Giảng viên:** + Giảng giải, đàm thoại làm rõ các nội dung. + Giải quyết các vấn đề an ninh mạng trong thực tiễn. + Giao nội dung thực hành. + Nhận xét đánh giá **- Sinh viên:** + Đọc trước tài liệu [1], [2] - chương 2 mục 2.1 – 2.4. + Lắng nghe, quan sát, ghi chép, thảo luận nhóm, trả lời câu hỏi. + Làm bài tập chương 2. + Đọc tài liệu tham khảo tài liệu [3] phần 2.	CĐR1.1 CĐR1.3 CĐR1.4
3.	**Chương III. An ninh mức giao vận và thư điện tử** **Mục tiêu chương:** Trình bày được vấn đề an ninh website, các giao thức SSL, TLS, chương trình PGP, chuẩn MIME, giao thức HTTPs và	16 (8LT, 8TH, 1KT)	**Thuyết trình, đàm thoại nêu vấn đề** **- Giảng viên:** + Giảng giải, đàm thoại làm rõ các nội dung. + Giải quyết các vấn đề an	CĐR1.1 CĐR1.3 CĐR2.1 CĐR3.1

TT	Nội dung giảng dạy	Số tiết	Phương pháp dạy-học	CĐR học phần
	giao thức SSH. **Nội dung cụ thể:** 3.1. Vấn đề an ninh website 3.2. Giao thức Secure Soctets Layer 3.3. Chuẩn Transport Layer Security 3.4. Giao thức Secure Shell 3.5. Chương trình Pretty Good Privacy 3.6. Chuẩn Multipurpose Internet Mail Extensions 3.7. Giao thức Hypertext Transfer Protocol Secure Bài thực hành chương 3 Báo cáo giữa học phần		ninh mạng trong thực tiễn. + Giao nội dung thực hành. + Nhận xét đánh giá. **- Sinh viên:** + Đọc trước tài liệu [1] - chương 3 mục 3.1 – 3.7. + Lắng nghe, quan sát, ghi chép, thảo luận nhóm, trả lời câu hỏi. + Làm bài tập chương 3. + Đọc tài liệu tham khảo tài liệu [3] phần 2. Sinh viên trình bày báo cáo giữa học phần	
4.	**Chương IV. An ninh và an toàn mạng máy tính** **Mục tiêu chương:** Trình bày được khái niệm lỗ hổng, các lỗ hổng bảo mật của mạng máy tính, một số lỗ hổng do người dùng vô tình gây ra, những vấn đề hackers và hậu quả hacker gây ra và các phương thức tấn công mạng qua lỗ hổng. **Nội dung cụ thể:** **4.1. Khái niệm lỗ hổng** 4.2. Các lỗ hổng bảo mật của hệ điều hành 4.3. Các lỗ hổng bảo mật của mạng máy tính 4.4. Một số lỗ hổng do người dùng vô tình gây ra 4.5. Hackers và hậu quả hacker gây ra **4.6. Tấn công mạng qua lỗ hổng** **Bài thực hành chương 4**	12 (6LT, 6TH)	**Thuyết trình, đàm thoại nêu vấn đề** **- Giảng viên:** + Giảng giải, đàm thoại làm rõ các nội dung. + Giải quyết các vấn đề an ninh mạng trong thực tiễn. + Giao nội dung thực hành. + Nhận xét đánh giá. **- Sinh viên:** + Đọc trước tài liệu [1] - chương 4 mục 4.1 – 4.6. + Lắng nghe, quan sát, ghi chép, thảo luận nhóm, trả lời câu hỏi. - Đọc tài liệu tham khảo tài liệu [2] Chương 3. + Làm bài tập chương 4.	CĐR1.1 CĐR1.2 CĐR1.3 CĐR2.1 CĐR3.1 CĐR3.2
5.	**Chương V. Một số kỹ thuật phát hiện xâm nhập và phòng thủ** **Mục tiêu chương:** Trình bày được một số kỹ thuật phòng thủ, hệ thống phát hiện xâm nhập IDS,	16 (8LT, 8TH)	**Thuyết trình, đàm thoại nêu vấn đề** **- Giảng viên:** + Giảng giải, đàm thoại làm rõ các nội dung.	CĐR1.1 CĐR1.2 CĐR1.3 CĐR1.4 CĐR2.1 CĐR2.2

TT	Nội dung giảng dạy	Số tiết	Phương pháp dạy-học	CĐR học phần
	phát hiện dấu hiệu không bình thường, các mẫu hành vi thông thường, phát hiện bất thường và một số kỹ thuật xử lý dữ liệu sử dụng trong các hệ thống phát hiện xâm nhập. **Nội dung cụ thể:** 5.1. Một số kỹ thuật phòng thủ 5.2. Hệ thống phát hiện xâm nhập IDS 5.3. Phát hiện dấu hiệu không bình thường 5.4. Các mẫu hành vi thông thường, phát hiện bất thường 5.5. Một số kỹ thuật xử lý dữ liệu sử dụng trong các hệ thống phát hiện xâm nhập Bài thực hành chương 5		+ Giải quyết các vấn đề an ninh mạng trong thực tiễn. + Giao nội dung thực hành. + Nhận xét đánh giá. **- Sinh viên:** + Đọc trước tài liệu [1] - chương 5 mục 5.1 –5.5. + Lắng nghe, quan sát, ghi chép, thảo luận nhóm, trả lời câu hỏi. + Làm bài tập chương 5. + Đọc tài liệu tham khảo tài liệu [3] phần 2.	CĐR3.1 CĐR3.2

Hải Dương, ngày 24 tháng 09 năm 2020

KT.HIỆU TRƯỞNG PHÓ HIỆU TRƯỞNG	KT.TRƯỞNG KHOA PHÓ TRƯỞNG KHOA	TRƯỞNG BỘ MÔN
TS. Nguyễn Thị Kim Nguyên	Phạm Văn Kiên	Phạm Văn Kiên