UBND TỈNH THÁI BÌNH
TRƯỜNG ĐẠI HỌC THÁI BÌNH

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

ĐỀ CƯƠNG CHI TIẾT HỌC PHẦN

AN TOÀN VÀ AN NINH MẠNG

Ngành đào tạo: Công nghệ thông tin

Bậc đào tạo: Đại học

(Ban hành kèm theo Quyết định số: 640/QĐ-ĐHTB, ngày 14/12/2019)

1. Tên học phần: An toàn và an ninh mạng – Mã học phần: IT5573073

2. Số tín chỉ: 3 (3,0)

3. Trình độ: Cho sinh viên năm thứ tư

4. Phân bổ thời gian

- Lên lớp:

Lý thuyết: 45 tiết (2 tiết lên lớp/tuần, 1 tiết = 50 phút)

Thực hành: 0 tiết

- Tự học: (45 x 2) = 90 giờ

5. Điều kiện tiên quyết: Học sau các học phần: Hệ điều hành, Mạng máy tính.

6. Mục tiêu của học phần

6.1. Kiến thức:

Mục tiêu của môn học là cung cấp cho sinh viên những kiến thức nền tảng về an toàn mạng trên cả hai khía cạnh: lý thuyết và thực tế. Môn học sẽ cung cấp một sự khảo sát toàn diện, cập nhật và thiết thực về các ứng dụng và các chuẩn an ninh.

6.2. Kỹ năng:

Hoàn thành môn học, sinh viên có thể hiểu được các mối đe dọa tiềm ẩn và nguồn gốc tấn công đối với an ninh mạng; từ đó chọn lựa những cơ chế an ninh phù hợp để ứng phó.

6.3. Về năng lực tự chủ và tự chịu trách nhiệm:

- Có thái độ nghiêm túc trong học tập;

- Có đạo đức, lương tâm nghề nghiệp, có trách nhiệm với công việc, dám làm, dám chịu trách nhiệm.

- Có ý thức tổ chức kỷ luật, chủ động trong quá trình học tập.

7. Mô tả vắn tắt nội dung của học phần:

Khái niệm về an toàn, an ninh mạng; Các phương pháp mã mật; Xác thực thông điệp, chữ ký điện tử và giao thức xác thực; An ninh hệ thống; An ninh trong mạng IP; An ninh trong các dịch vụ Internet; Tường lửa.

8. Nhiệm vụ của sinh viên:

- Lên lớp theo quy chế (Lên lớp ≥ 80% số tiết của học phần).
- Hoàn thành bài tập giáo viên giao.
- Bài tập tiểu luận môn học.
- Dự kiểm tra học trình và thi hết học phần.

9. Tài liệu học tập:

- Sách, giáo trình chính:

[1] Giáo trình An toàn và an ninh mạng-Trường Đại học Thái Bình.

-Tài liệu tham khảo:

[2] *Cryptography and Network Security,* W. Stallings, 4th ed., Prentice Hall, 2005.

[3] Sybex - CompTIA Security+ Deluxe Study Guide.Nov.2008

[4] Network Security: A Beginner's Guide, Eric Maiwald, 2nd ed., McGraw-Hill Osborne Media, 2003.

10. Tiêu chuẩn đánh giá sinh viên: Theo quy chế số 25/2006/QĐ-BGDĐT ngày 26/6/2006 của Bộ trưởng Bộ Giáo dục và Đào tạo.

10.1. Thang điểm đánh giá: 10

10.1. Tiêu chí đánh giá

STT	Điểm thành phần	Quy định	Trọng số	Ghi chú
1	Điểm thường xuyên, đánh giá nhận thức, thái độ thảo luận, chuyên cần, làm bài tập ở nhà.	- Số tiết dự học/Tổng số tiết: 10%. - Số bài tập đã làm/Tổng số bài tập được giao: 10%.	20%	
2	Điểm kiểm tra định kỳ 3 điểm Kiểm tra viết 50’ Điểm tiểu luận	- 2 bài kiểm tra 1 tiết trên lớp. - 1 điểm tiểu luận	30%	
3	Thi kết thúc học phần	- Thi lý thuyết (90’)	50%	

10.2. Cách tính điểm

- Sinh viên không tham gia đủ 80% số tiết học trên lớp không được thi lần đầu.

- Điểm thành phần để điểm lẻ đến một chữ số thập phân.

- Điểm kết thúc học phần làm tròn đến 0.5.

11. Thang điểm: 10

12. Nội dung chi tiết học phần

Chương	Nội dung	LT	TH
1	**Chương 1: Tổng quan về an toàn và an ninh thông tin** 1.1 Mở đầu 1.2 Thành phần của một hệ thống thông tin 1.3 Những mối đe dọa và thiệt hại đối với hệ thống thông tin. 1.4 Các kiểu tấn công 1.5 Các lỗ hổng bảo mật 1.6 Giải pháp điều khiển kiểm soát an toàn bảo mật	6	0
2	**Chương 2: Mã hóa đối xứng và bảo mật thông tin** 2.1 Nguyên tắc mã hóa đối xứng 2.2 Các giải thuật mã hóa đối xứng 2.3 Các chế độ mã hóa 2.4 Vị trí thiết bị mã hóa 2.5 Vấn đề phân phối khóa trong mã hóa đối xứng	4	0
3	**Chương 3: Mã hóa khóa công khai và chứng thực thông t** 3.1 Giới thiệu về chứng thực thông tin 3.2 Các hàm băm và giải thuật HMAC 3.3 Nguyên lý mã hóa khóa công khai 3.4 Các giải thuật mã hóa khóa công khai 3.5 Chữ ký số 3.6 Quản lý khóa	5+1 KT	0
4	**Chương 4: Các ứng dụng xác thực** 4.1 Xác thực đơn, đa yếu tố 4.2 Kerberos – một dịch vụ xác thực khóa bí mật 4.3 X.509 – một dịch vụ xác thực khóa công khai 4.4 PKI – hạ tầng khóa công khai	4	0

Chương	Nội dung	LT	TH
5	**Chương 5: IP Security** 5.1 Giới thiệu 5.2 Kiến trúc IP Security 5.3 Authentication Header 5.4 Encapsulation Security Payload 5.5 Kết hợp Security Associations 5.6 Quản lý khóa 5.7 VPN	5 + 1KT	0
6	**Chương 6: Phần mềm mã độc** 6.1 Mã độc 6.2 Các biện pháp đối phó với mã độc	4	0
7	**Chương 7: Bảo mật Web** 7.1 Đặt vấn đề 7.2 Secure Socket Layer và Transport Layer Security 7.3 Secure Electronic Transaction 7.4 Pretty Good Privacy 7.5 S/MIME 7.6 Các vấn đề bảo mật trong dịch vụ Email	8	0
8	**Chương 8: Kiểm soát truy nhập** 8.1 Mô hình access control 8.2 Rủi ro và quy trình khôi phục rủi ro an ninh 8.3 Chính sách an ninh 8.4 Hệ thống tin cậy	4	0
9	**Chương 9: Firewalls** 9.1 Khái niệm firewalls 9.2 Chức năng của firewall 9.3 Phân loại 9.4 Nguyên lý thiết kế Firewalls 9.5 Các bước cần thiết xây dựng firewall Ôn tập kết thúc	3	0

13. Hình thức và nội dung từng tuần:

HTTCDH	Nội dung	Thời gian (tiết)	Yêu cầu SV chuẩn bị và địa chỉ tư liệu	Ghi chú
Nội dung: *(Tuần 1)*				
Lý thuyết	**Chương 1: Tổng quan về an toàn và an ninh thông tin** 1.1 Mở đầu 1.2 Thành phần của một hệ thống thông tin 1.3 Những mối đe dọa và thiệt hại đối với hệ thống thông tin. 1.4 Các kiểu tấn công 1.5 Các lỗ hổng bảo mật	4	Tài liệu [1] Chương 1 Tài liệu [2]. Chương 1	
Nội dung: *(Tuần 2)*				
Lý thuyết	1.6 Giải pháp điều khiển kiểm soát an toàn bảo mật **Chương 2: Mã hóa đối xứng và bảo mật thông tin** 2.1 Nguyên tắc mã hóa đối xứng 2.2 Các giải thuật mã hóa đối xứng	4	Tài liệu [1] Chương 1,2 Tài liệu [3].	
Nội dung: *(Tuần 3)*				
Lý thuyết	2.3 Các chế độ mã hóa 2.4 Vị trí thiết bị mã hóa 2.5 Vấn đề phân phối khóa trong mã hóa đối xứng **Chương 3: Mã hóa khóa công khai và chứng thực thông tin** 3.1 Giới thiệu về chứng thực thông tin 3.2 Các hàm băm và giải thuật HMAC	4	Tài liệu [1] Chương 2,3 Tài liệu [2]. Tài liệu [4].	
Nội dung: *(Tuần 4)*				
Lý thuyết	3.3 Nguyên lý mã hóa khóa công khai 3.4 Các giải thuật mã hóa khóa công khai 3.5 Chữ ký số 3.6 Quản lý khóa	3 + 1KT	Tài liệu [1] chương 3 Tài liệu [4].	
Nội dung: *(Tuần 5)*				

HTTCDH	Nội dung	Thời gian (tiết)	Yêu cầu SV chuẩn bị và địa chỉ tư liệu	Ghi chú
Lý thuyết	**Chương 4: Các ứng dụng xác thực** 4.1 Xác thực đơn, đa yếu tố 4.2 Kerberos – một dịch vụ xác thực khóa bí mật 4.4 X.509 – một dịch vụ xác thực khóa công khai 4.4 PKI – hạ tầng khóa công khai	4	Tài liệu [1] Chương 4 Tài liệu [3].	
Nội dung: *(Tuần 6)*				
Lý thuyết	**Chương 5: IP Security** 5.1 Giới thiệu 5.2 Kiến trúc IP Security 5.3 Authentication Header 5.4 Encapsulation Security Payload 5.5 Kết hợp Security Associations	4	Tài liệu [1] Chương 5 Tài liệu [2].	
Nội dung: *(Tuần 7)*				
Lý thuyết	5.6 Quản lý khóa 5.7 VPN **Chương 6: Phần mềm mã độc** 6.1 Mã độc	LT: 3 KT: 1	Tài liệu [1] Chương 5,6 Tài liệu [3].	
Nội dung: *(Tuần 8)*				
Lý thuyết	6.2 Các biện pháp đối phó với mã độc **Chương 7: Bảo mật Web** 7.1 Đặt vấn đề 7.2 Secure Socket Layer và Transport Layer Security	4	Tài liệu [1] Chương 6,7 Tài liệu [2].	
Nội dung: *(Tuần 9)*				
Lý thuyết	7.3 Secure Electronic Transaction 7.4 Pretty Good Privacy	4	Tài liệu [1] Chương 7 Tài liệu [4].	
Nội dung: *(Tuần 10)*				

HTTCDH	Nội dung	Thời gian (tiết)	Yêu cầu SV chuẩn bị và địa chỉ tư liệu	Ghi chú
Lý thuyết	7.5 S/MIME 7.6 Các vấn đề bảo mật trong dịch vụ Email **Chương 8: Kiểm soát truy nhập** 8.1 Mô hình access control 8.2 Rủi ro và quy trình khôi phục rủi ro an ninh	4	Tài liệu [1] Chương 7,8 Tài liệu [4].	
Nội dung: *(Tuần 11)*				
Lý thuyết	8.3 Chính sách an ninh 8.4 Hệ thống tin cậy **Chương 9: Firewalls** 9.1 Khái niệm firewalls 9.2 Chức năng của firewall 9.3 Phân loại	4	Tài liệu [1] Chương 8,9 Tài liệu [2].	
Nội dung: *(Tuần 12)*				
Lý thuyết	9.4 Nguyên lý thiết kế Firewalls 9.5 Các bước cần thiết xây dựng firewall Ôn tập kiểm tra.	2	Tài liệu [1] Chương 9 Tài liệu [3].	

TRƯỞNG KHOA
(Đã ký)

TRƯỞNG BỘ MÔN
(Đã ký)