

**CHƯƠNG TRÌNH CHI TIẾT HỌC PHẦN
TRÌNH ĐỘ ĐẠI HỌC**

**Ngành/chuyên ngành đào tạo: Mạng máy tính; Công nghệ phần mềm;
Hệ thống thông tin**

- 1. Tên học phần: Đảm bảo và An toàn thông tin**
- 2. Loại học phần:** Lý thuyết, thực hành
- 3. Số tín chỉ:** 03 tín chỉ. Trong đó LT 02 tín chỉ, thực hành: 01 tín chỉ
- 4. Bộ môn quản lý học phần:** Mạng và Công nghệ phần mềm
- 5. Điều kiện tiên quyết:** Môn học trước: Mạng máy tính
- 6. Phân bổ thời gian**
 - Thời gian trên lớp: 60 tiết
 - Số tiết lý thuyết: 30 tiết;
 - Số tiết thực hành: 27 tiết;
 - Số tiết kiểm tra: 03 tiết;
 - Thời gian tự học: 90 tiết
- 7. Mục tiêu của học phần**

7.1. Kiến thức

- Nắm rõ cơ sở luật pháp, chính sách an ninh mạng, quản lý rủi ro, quá trình xây dựng hệ thống an toàn, vấn đề an toàn hệ thống và an ninh mạng trong thực tiễn;
- Hiểu và vận dụng được một số kỹ thuật và công nghệ an ninh mạng phổ biến hiện nay như: tường lửa, mạng riêng ảo, hệ thống phát hiện xâm nhập, an toàn cho các thiết bị đơn và nối mạng Internet;
- Nắm được tổng quan về mục tiêu của an toàn và bảo mật hệ thống thông tin. Nắm rõ một số hiện trạng về tình hình an toàn và bảo mật hệ thống thông tin hiện tại;
- Một số vấn đề cần quan tâm trong an toàn và bảo mật hệ thống thông tin cũng như các chính sách, tiêu chuẩn, chỉ dẫn trong an toàn bảo mật hệ thống thông tin;
- Tìm hiểu các mô hình mã hóa, các kỹ thuật mã hóa và các đánh giá liên quan đến thời gian mã hóa, và phá mã. Hiểu rõ các thành phần của một hệ mật mã, các thuật toán mã hóa cổ điển, hiện đại cũng như cung cấp những yếu tố bảo mật then chốt như xác thực, tính toàn vẹn và không thu hồi;
- Hiểu tính năng của một số phần mềm ác tính cũng như biết một số biện pháp phòng chống, ngăn chặn. Biết phân tích một số lỗi phần mềm từ đó đưa ra các giải pháp ngăn chặn;
- Phân tích được các nguy cơ và lỗ hổng tiềm tàng đối với an toàn hệ điều hành Windows, Ubuntu, Linux cũng như hiểu rõ những hiểm họa, các mối đe dọa tiềm ẩn có thể xảy ra đối với CSDL, đồng thời biết những giải pháp có thể sử dụng để bảo vệ CSDL đối với những hiểm họa;

- Xác định tất cả những nguyên nhân dẫn đến dữ liệu trên máy tính bị mất. Phân tích những nguyên nhân đưa đến việc rò rỉ thông tin, sử dụng được các thiết bị lưu trữ thông dụng;

- Sao lưu dữ liệu dưới nhiều hình thức. Phục hồi dữ liệu trong một số trường hợp; Hiểu rõ đặc điểm của kiểm soát truy nhập MAC và DAC trong CSDL;

- Hiểu các kiến thức cơ bản về truyền thông mạng, an ninh mạng, các nguy cơ và hiểm họa tiềm ẩn, xác định và ngăn chặn tấn công; bảo mật hệ thống cá nhân, đảm bảo giao dịch truyền dữ liệu, đảm bảo an ninh cá nhân qua mail, truy nhập Internet. Nghiên cứu và tìm hiểu các khái niệm, nguyên tắc cơ bản trong an ninh mạng máy tính.

7.2. Kỹ năng

- Vận dụng các phương pháp mã hóa để ứng dụng trong các giao thức mạng phục vụ mục đích đảm bảo an toàn cho truyền thông tin;

- Áp dụng một cách thích hợp các kỹ thuật căn bản đảm bảo an toàn truyền thông và an toàn hệ thống khi bị tấn công trên mạng;

- Có kỹ năng xây dựng các giải pháp đảm bảo an ninh của các hệ thống mạng cũng như nguy cơ, các dạng tấn công và một số kỹ thuật xâm nhập hệ thống mạng;

- Khai thác có hiệu quả và sử dụng thành thạo một số phần mềm, công cụ để ngăn chặn, phân tích và xử lý một số phần mềm độc hại tấn công vào hệ thống thông tin;

- Xây dựng được các mô hình CSDL tập trung, phân tán, Server/Client cũng như kiểm soát được các luồng dữ liệu;

- Sử dụng được một số phần mềm tiện ích và phần mềm công cụ để phục hồi, bảo vệ cho hệ thống thông tin;

- Có khả năng ứng dụng các giải pháp kỹ thuật trong các ứng dụng bảo vệ mạng máy tính. Xây dựng được một hệ thống phát hiện xâm nhập bất hợp pháp trên hệ thống; Thực hiện được tấn công và phòng chống tấn công trên các trang Website.

7.3. Thái độ

+ Có ý thức và tinh thần trách nhiệm, thái độ và đạo đức đúng đắn, ý thức kỷ luật và tác phong công nghiệp để đáp ứng yêu cầu thực tế mà công việc đòi hỏi;

+ Có phương pháp làm việc khoa học, khả năng làm việc độc lập, làm việc theo nhóm, khả năng tự nghiên cứu và nâng cao chất lượng học tập;

+ Có tinh thần trách nhiệm với bản thân và tập thể, tinh thần học hỏi, ý trí vươn lên để hoàn thiện bản thân để tiếp tục học tập ở các trình độ cao hơn.

8. Nội dung học phần

8.1. Mô tả vắn tắt

Học phần gồm 6 chương. Chương 1. Giúp sinh viên hiểu rõ các khái niệm căn bản, các mô hình về an toàn hệ thống thông tin. Chương 2. Giúp sinh viên biết được công việc của chuyên gia đảm bảo an toàn hệ thống, đồng thời nắm được cơ sở về các hệ mã mật (cổ điển, hiện đại), Chương 3. An toàn phần mềm cũng như biết đánh giá

độ an toàn và một số ứng dụng của mã mật, Chương 4. Triển khai một chương trình an toàn bảo mật trên hệ điều hành. Chương 5. Có khả năng đánh giá độ tin cậy, xác định các lỗ hổng bảo mật, đe dọa và xây dựng các chính sách bảo mật, các nguy cơ đối với một hệ thống thông tin. Chương 6. Hiểu được các thông tin về tấn công và các giải pháp cũng như các kỹ thuật để đảm bảo an toàn thông tin, mạng máy tính cũng như một số kỹ thuật phát hiện xâm nhập bất hợp pháp vào hệ thống thông tin.

8.2. Nội dung chi tiết học phần

Tuần	NỘI DUNG	LT (tiết)	TH (tiết)	Tài liệu đọc trước	Nhiệm vụ của sinh viên
1	Chương 1. Tổng quan về an toàn thông tin 1.1. Khái niệm về An toàn hệ thống thông tin 1.2. Các mục tiêu an toàn 1.3. Các mối đe dọa	2	2	Tài liệu [1] Chương 1 (Từ 1.1 đến 1.3)	- Nghe giảng, đọc trước nội dung trong tài liệu [1] Chương 1 từ 1.4 đến 1.6 - Làm bài tập cuối chương 1 - Thực hành theo tài liệu số [2] tuần 1
2	1.4. Quản lý các nguy cơ mất an toàn trên HTTT 1.5. Quản lý các nguy cơ mất ATTT 1.6. Các giải pháp đảm bảo ATTT	2	2	Tài liệu [1] Chương 1 (Từ 1.4 đến 1.6)	- Nghe giảng, đọc trước nội dung trong tài liệu [1] Chương 2 từ 2.1 đến 2.2 - Làm bài tập cuối chương 1 - Thực hành theo tài liệu số [2] tuần 2
3	Chương 2. Mã hóa dữ liệu và ứng dụng 2.1. Các khái niệm cơ bản về mật mã 2.2. Một số hệ mật mã cổ điển	2	2	Tài liệu [1] Chương 2 (Từ 2.1 đến 2.2)	- Nghe giảng, đọc trước nội dung trong tài liệu [1] Chương 2 từ 2.3 đến 2.5 - Làm bài tập cuối chương 2 - Thực hành theo tài liệu số [2] tuần 3
4	2.3. Mật mã khóa đối xứng 2.4. Mật mã khóa công khai 2.5. Hàm băm	2	2	Tài liệu [1] Chương 2 (Từ 2.3 đến 2.5)	- Nghe giảng, đọc trước nội dung trong tài liệu [1] Chương 2 từ 2.6 đến 2.9 - Làm bài tập cuối chương 2

COM
 TP
 Đ.
 :ON
 QU
 /

					- Thực hành theo tài liệu số [2] tuần 4
5	2.6. Chữ ký số 2.7. Quản lý khóa 2.8. Chứng thực 2.9. Giao thức mật mã và ứng dụng	2	1	Tài liệu [1] Chương 2 (Từ 2.6 đến 2.9)	- Nghe giảng, đọc trước nội dung trong tài liệu [1] Chương 3 từ 3.1 đến 3.2 - Làm bài tập cuối chương 3 - Thực hành theo tài liệu số [2] tuần 5
	Kiểm tra bài số 1		1		Làm bài kiểm tra số 1
6	Chương 3. An toàn phần mềm 3.1. Phần mềm ác tính 3.2. Các biện pháp ngăn chặn phần mềm ác tính	2	2	Tài liệu [1] Chương 3 (Từ 3.1 đến 3.2)	- Nghe giảng, đọc trước nội dung trong tài liệu [1] Chương 3 từ 3.3 đến 3.5 - Làm bài tập cuối chương 3 - Thực hành theo tài liệu số [2] tuần 6
7	3.3. Lỗi phần mềm 3.4. Các biện pháp ngăn chặn: Kiểm thử; Kiểm định; Lập trình an toàn 3.5. Dịch vụ an toàn hệ thống thông tin	2	2	Tài liệu [1] Chương 3 (Từ 3.3 đến 3.5)	- Nghe giảng, đọc trước nội dung trong tài liệu [1] Chương 4 từ 4.1 đến 4.3 - Làm bài tập cuối chương 3 - Thực hành theo tài liệu số [2] tuần 7
8	Chương 4. An toàn hệ điều hành 4.1. Vai trò và Các vấn đề bảo vệ trong hệ điều hành 4.2. Một số mô hình toán học bảo mật hệ điều hành 4.3. Bảo vệ, Quản lý bộ nhớ và địa chỉ	2	2	Tài liệu [1] Chương 4 (Từ 4.1 đến 4.3)	- Nghe giảng, đọc trước nội dung trong tài liệu [1] Chương 4 từ 4.4 đến 4.7 - Làm bài tập cuối chương 4 - Thực hành theo tài liệu số [2] tuần 8
9	4.4. Quản lý người dùng; Xác thực 4.5. Bảo vệ và Quản lý tệp 4.6. Điều khiển truy nhập	2	2	Tài liệu [1] Chương	- Nghe giảng, đọc trước nội dung trong tài liệu

IG
RUC
AI H
GN
NG
★

	4.7. Nguyên tắc thiết kế hệ điều hành tin cậy			4(Từ 4.4 đến 4.7)	[1] Chương 5 từ 5.1 đến 5.4 - Làm bài tập cuối chương 4 - Thực hành theo tài liệu số [2] tuần 9
10	Chương 5. An toàn cơ sở dữ liệu 5.1. Tổng quan về An toàn CSDL 5.2. Dữ liệu nhạy cảm 5.3. Thiết kế CSDL an toàn 5.4. Các mối đe dọa khác	2	1	Tài liệu [1] Chương 5(Từ 5.1 đến 5.4)	- Nghe giảng, đọc trước nội dung trong tài liệu [1] Chương 5 từ 5.5 đến 5.8 - Làm bài tập cuối chương 5 - Thực hành theo tài liệu số [2] tuần 10
	Kiểm tra bài số 2		1		Làm bài kiểm tra số 2
11	5.5. Cơ sở dữ liệu đa tầng 5.6. Thống kê CSDL 5.7. Xây dựng kế hoạch sao lưu dữ liệu trên máy tính đơn 5.8. Xây dựng kế hoạch sao lưu dữ liệu trên máy tính có nối mạng Internet	2	2	Tài liệu [1] Chương 5(Từ 5.5 đến 5.8)	- Nghe giảng, đọc trước nội dung trong tài liệu [1] Chương 6 từ 6.1 đến 6.4 - Làm bài tập cuối chương 5 - Thực hành theo tài liệu số [2] tuần 11
12	Chương 6. An toàn Internet 6.1. Tổng quan về an toàn mạng 6.2. Các mối đe dọa trên mạng và internet 6.3. Các phương thức điều khiển truy nhập mạng máy tính 6.4. Các biện pháp ngăn chặn	2	2	Tài liệu [1] Chương 6(Từ 6.1 đến 6.4)	- Nghe giảng, đọc trước nội dung trong tài liệu [1] Chương 6 từ 6.4 đến 6.6 - Làm bài tập cuối chương 6 - Thực hành theo tài liệu số [2] tuần 12
13	6.5. Công nghệ tường lửa 6.6. Hệ thống phát hiện xâm nhập	2	2	Tài liệu [1] Chương 6(Từ 6.5 đến 6.6)	- Nghe giảng, đọc trước nội dung trong tài liệu [1] Chương 6 từ 6.7 đến 6.8 - Làm bài tập cuối chương 6 - Thực hành theo tài liệu số [2] tuần

NG
OC
3H
NIM

					13
14	6.7. Tấn công 6.8. An toàn thư điện tử	2	2	Tài liệu [1] Chương 6 (Từ 6.7 đến 6.8)	- Nghe giảng, đọc trước nội dung trong tài liệu [1] Chương 6 từ 6.9 đến 6.10 - Làm bài tập cuối chương 6 - Thực hành theo tài liệu số [2] tuần 14
15	6.9. Các cơ chế đảm bảo an toàn thông tin IPSEC; SSL; SET 6.10. An ninh mạng WLAN	2	1	Tài liệu [1] Chương 6 (Từ 6.9 đến 6.10)	- Làm bài tập cuối chương 6 - Thực hành theo tài liệu số [2] tuần 15
	Kiểm tra bài số 3		1		Làm bài kiểm tra số 3
	Tổng cộng	30	30		

9. Nhiệm vụ của sinh viên

- Dự lớp: Tối thiểu 70% số giờ học trên lớp có sự hướng dẫn của giảng viên;
- Bài tập, thực hành:
 - + Làm bài tập và trả lời các câu hỏi đầy đủ;
 - + Đọc thêm tài liệu giảng viên yêu cầu;
 - + Đưa ra những câu hỏi liên quan đến môn học để thảo luận;
 - + Thi kiểm tra giữa kỳ và thi kiểm tra kết thúc học phần.

10. Thang điểm và hình thức đánh giá:

- **Thang điểm:** Thang điểm 10 (từ 0 - 10)

- **Hình thức đánh giá:**

- Sinh viên không tham gia đủ 70% số tiết học trên lớp không được dự thi kết thúc học phần và nhận điểm 0;
- Điểm thành phần để điểm lẻ đến một chữ số thập phân;
- Điểm học phần làm tròn đến phần nguyên.

11. Tiêu chuẩn đánh giá sinh viên

TT	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: 5% - Số bài tập đã làm/tổng số bài tập được giao và tham gia thảo luận trên lớp: 5%	10%	
2	Điểm kiểm tra giữa kỳ	- Hình thức KT: Thực hành trên máy tính. - Số lượng bài KT: 03	30%	50 phút/bài
3	Thi kết thúc học phần	Hình thức thi: Hỗn hợp (Vấn đáp + thực hành)	60%	60 phút

12. Tài liệu học tập

- Giáo trình bắt buộc

[1] Bài giảng Đảm bảo và an toàn thông tin, Bộ môn Mạng & CNPM biên soạn và cập nhật năm 2019;

[2]. Tài liệu thực hành Đảm bảo và an toàn thông tin, Bộ môn Mạng & CNPM biên soạn và cập nhật năm 2019;

- Tài liệu tham khảo

[1] William Stallings. Network Security Essentials: Applications and Standards, Third Edition. Prentice Hall, 2007.

[2] Thomas R. Peltier, Justin Peltier, John Blackley, *Information Security Fundamentals*, AUERBACH, 2004.

[3] Harold F. Tipton, Micki Krause, *Information Security Management Handbook 5th*, CRC Press, 2004

13. Các yêu cầu khác (nếu có) của học phần:

Quảng Ninh, ngày 02 tháng 3 năm 2020



HIỆU TRƯỞNG

TS. Hoàng Hùng Thắng

TRƯỞNG BỘ MÔN

ThS. Đặng Đình Đức

GIẢNG VIÊN BIÊN SOẠN

ThS. Đặng Đình Đức

THƯƠNG