HỌC VIỆN KỸ THUẬT QUÂN SỰ
KHOA.....

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

ĐỀ CƯƠNG CHI TIẾT HỌC PHẦN
AN TOÀN VÀ BẢO MẬT HỆ THỐNG THÔNG TIN

1. Thông tin về giáo viên

TT	Họ tên giáo viên	Học hàm	Học vị	Đơn vị công tác (Bộ môn)
1	Nguyễn Mậu Uyên	GVC	Th.S	Hệ thống thông tin
2	Tống Minh Đức	GVC	TS	Hệ thống thông tin

Thời gian, địa điểm làm việc: Các ngày trong tuần tại phòng làm việc bộ môn A1505

Địa chỉ liên hệ: Bộ môn Hệ thống Thông tin, Khoa Công nghệ Thông tin, Học viện Kỹ thuật Quân sự.

Điện thoại, email: 0983602237 - 0984485888 Email: nguyenitt2005@gmail.com; tmduc08@gmail.com

Các hướng nghiên cứu chính: Xử lý ảnh, an toàn bảo mật hệ thống thông tin, tính toán thông minh.

2. Thông tin chung về học phần

- Tên học phần: Đảm bảo và an toàn thông tin.
- Mã học phần: 12322151
- Số tín chỉ: 03
- Học phần (bắt buộc hay lựa chọn):
- Các học phần tiên quyết:
- Các yêu cầu đối với học phần (nếu có):
- Giờ tín chỉ đối với các hoạt động:
  - Nghe giảng lý thuyết: 45 tiết
  - Làm bài tập trên lớp: 15 tiết
  - Thảo luận:
  - Thực hành, thực tập (ở PTN, nhà máy, thực tập...):
  - Hoạt động theo nhóm:
  - Tự học: 45 tiết
- Khoa/Bộ môn phụ trách học phần, địa chỉ: Bộ môn Hệ thống Thông tin, Khoa Công nghệ Thông tin, Học viện Kỹ thuật Quân sự.

3. Mục tiêu của học phần

- Kiến thức: Kiến thức về các nguy cơ với một hệ thống thông tin, các tài liệu về triển khai chương trình an toàn bảo mật hệ thống thông tin. Thông tin về tấn công và giải pháp kỹ thuật để đảm bảo an toàn mạng máy tính, đảm bảo truyền thông tin mạng máy tính.
- Kỹ năng: Tìm hiểu tài liệu, mô hình đề xuất phương án giải quyết.
- Thái độ, chuyên cần: Yêu cầu chú ý nghe giảng trên lớp, tích cực nghiên cứu tài liệu ở nhà và tham gia thảo luận, làm bài tập, thí nghiệm theo yêu cầu.

4. Tóm tắt nội dung học phần *(khoảng 150 từ)*

Giới thiệu các nguy cơ với một hệ thống thông tin bao gồm về kỹ thuật và các vấn đề về quản lý, con người. Những vấn đề cần chú ý khi xây dựng chính sách, tiêu chuẩn về an toàn và bảo mật hệ thống thông tin. Qui trình và các điểm chú ý khi xây dựng một chương trình bảo đảm an toàn bảo mật hệ thống thông tin, một số chính sách điển hình trong hệ thống thông tin. Một số vấn đề kỹ thuật liên quan đến tấn công mạng máy tính, các lỗi tiềm tàng của lập trình viên trong tấn công các ứng dụng được phát triển, và bảo mật mạng máy tính. Các kỹ thuật mã hóa tiêu biểu và vấn đề đảm bảo an toàn thông tin trong lưu trữ và truyền thông tin trên mạng máy tính.

5. Nội dung chi tiết học phần *(tên các chương, mục, tiểu mục)*

Chương, mục, tiểu mục	Nội dung	Số tiết	Giáo trình, Tài liệu tham khảo (TT của TL ở mục 6)	Ghi chú
Phần I.	**Lý thuyết**	**30**		
Chương 1.	**Tổng quan về an toàn bảo mật hệ thống thông tin**	**3**		
1.1	Vấn đề về an toàn và bảo mật hệ thống thông tin – Thông tin – Phạm vi hệ thống thông tin – Đảm bảo và an toàn thông tin			
1.2	Phạm vi vấn đề, một số nhìn nhận về an toàn bảo mật thông tin – Phạm vi đảm bảo và an toàn thông tin – Một số khái niệm liên quan			
1.3	Mục tiêu an toàn bảo mật hệ thống thông tin – Mô hình tam giác mục tiêu – Phân tích chi tiết các mục tiêu – Minh họa tương ứng mục tiêu và các vấn đề trong thực tiễn			
1.4.	Các khái niệm			
1.5	Các nguồn nguy cơ với hệ thống thông tin			
1.6.	Các loại đe dọa với hệ thống thông tin			
1.7.	Quy trình quản lý nguy cơ			
1.8.	Giải pháp đảm bảo an toàn và bảo mật hệ thống thông tin			
Chương 2.	**Phân tích đánh giá nguy cơ về an toàn bảo mật hệ thông thông tin**	**6**		
2.1	Các nhóm nguy cơ và đánh giá			

Chương, mục, tiểu mục	Nội dung	Số tiết	Giáo trình, Tài liệu tham khảo (TT của TL ở mục 6)	Ghi chú
2.2.	Những đe dọa từ nhân tố con người – Giới thiệu các đe dọa đến từ nhân tố con người: bỏ quyên, lỗi, trộm cắp, …			
2.3.	Những đe dọa đến từ nhân tố kỹ thuật – Tấn công mang tính kỹ thuật: tấn công mạng máy tính, tấn công mã độc			
2.4.	Kết hợp nhân tố con người và nhân tố kỹ thuật trong tấn công hệ thống – Tấn công social engeneering			
2.5.	Các đe dọa khác – Lỗi thiết thiết bị – Các vấn đề tai họa, thiên tai			
Chương 3.	**Giải pháp an toàn bảo mật hệ thông thông tin**	**15**		
3.1	Vấn đề an toàn bảo mật và chính sách – Phân tích sự cần thiết phải có chính sách, tiêu chuẩn, chỉ dẫn và chương trình an toàn bảo mật hệ thống thông tin – Một số chính sách tiêu biểu – Kế hoạch công việc liên tục – Một số minh họa về chính sách phân lớp thông tin và quản lý tài liệu	3		
3.2	Vấn đề về an toàn bảo mật và mã hóa – Sự quan trọng của mã hóa trong an toàn và bảo mật thông tin – Mô hình mã hóa thông tin, và đánh giá (mã hóa cổ điển, mã hóa tiêu chuẩn mới, mã hóa công khai, hàm băm) – Mô hình triển khai mã hóa trong lưu trữ và truyền thông tin – Mô hình triển khai dịch vụ dựa trên mô hình mã hóa (chữ ký số, xác thực số, …)	6		
3.3.	Vấn đề an toàn bảo mật và mạng máy tính	**3**		

Chương, mục, tiểu mục	Nội dung	Số tiết	Giáo trình, Tài liệu tham khảo (TT của TL ở mục 6)	Ghi chú
	– Giải pháp chống tấn công mạng máy tính bằng thiết bị – Giải pháp chống tấn công mạng máy tính bằng sử dụng phần mềm, chuẩn mới – Giải pháp chống mã độc			
3.4.	Vấn đề an toàn bảo mật hệ thống thông tin trong phát triển phần mềm – Một số vấn đề lỗi trong phát triển phần mềm – Quy trình phát triển phần mềm an toàn – Một số vấn đề phát triển phần mềm an toàn	3		
Chương 4.	**Quy chuẩn về an toàn bảo mật hệ thống**	**3**		
4.1	Giới thiệu về tiêu chuẩn an toàn và bảo mật cho hệ thống thông tin: ISO 27001, …			
Chương 5.	**Đánh giá an toàn bảo mật hệ thống, dịch vụ an toàn hệ thống**	**3**		
5.1.	Giới thiệu các công cụ đánh giá an toàn và bảo mật hệ thống thông tin			
5.2.	Giới thiệu các phương thức phát hiện tấn công			
5.3.	Phương thức điều tra tội phạm			
Phần II	**Vấn đề triển khai thực tiễn**	**30**		
Chủ đề 1.	Xây giải pháp triển khai mã hóa cho cơ sở dữ liệu, truyền dữ liệu – Sinh viên có mô hình về hệ thống, bao gồm cơ sở dữ liệu, các dịch vụ hoạt động – Đánh giá mức độ quan trọng của dữ liệu hệ thống – Lựa chọn phương thức mã hóa, dịch vụ mã hóa để đảm bảo cơ sở dữ liệu, các dịch vụ cung cấp của hệ thống an toàn	6		

Chương, mục, tiểu mục	Nội dung	Số tiết	Giáo trình, Tài liệu tham khảo (TT của TL ở mục 6)	Ghi chú
Chủ đề **2**	Phân tích lỗi của hệ thống phần mềm (mẫu), lỗi về ứng dụng, lỗi về web – Sinh viên tiếp cận một trong hai mô hình phần mềm là ứng dụng trên desktop, và hệ thống web site – Từ chương trình triển khai đánh giá sự tồn tại lỗi khả năng bị tấn công của hệ thống – Từ mã nguồn đánh giá khả năng bị tấn công của hệ thống	6		
Chủ đề 3	Một số vấn đề về đảm bảo cho hệ thống thông tin – Tổ chức, hoạt động, khởi tạo các phần mềm, quy trình đảm bảo – Tài nguyên cho vấn đề đảm bảo – Một số triển khai vấn đề đảm bảo	6		
Chủ đề 4	Xây dựng quy định về sử dụng ứng dụng, và quy trình đảm bảo an toàn cho hệ thống (mẫu) – Yêu cầu sinh viên đề ra các yêu cầu để đảm bảo an toàn bảo mật hệ thống thông tin cho cho việc phát triển một hệ thống (từ bảo mật cơ sở dữ liệu, truyền dữ liệu, phân quyền, quy định sử dụng phần mềm, chính sách về backup, các kế hoạch công việc liên tục tương ứng với hệ thống)	6		
Chủ đề **5**	Mô hình tấn công hệ thống – Cho một hệ thống thực tế, tấn công hệ thống với công cụ, kiến thức có được, phát triển công cụ, hoặc mở rộng các công cụ, phương thức tấn công mới với hệ thống.	6		

6. Giáo trình, tài liệu tham khảo

	Tên tài liệu	Tình trạng tài liệu

TT		Có ở thư viện	Giáo viên có hoặc khoa có	Đề nghị mua mới	Đề nhị biên soạn mới
1	Thomas R. Peltier, Justin Peltier, John Blackley, *Information Security Fundamentals*, AUERBACH, 2004.		×		
2	Douglas Stinson, *Cryptography: Theory and Practice*, CRC Press, 1995.		×		
3	Ed Skoudis, Lenny Zeltser, *Malware: Fighting Malicious Code*, Prentice Hall PTR, 2003.		×		
4	Michael Cross, *Developer's Guide to Web Application Security*, Syngress,		×		
5	Michael Howard, David LeBlanc and John Viega , *19 Deadly Sins of Software Security: Programming Flaws and How to Fix Them*, McGraw-Hill, 2005		×		
6	Justin Clarke, Nitesh Dhanjani, *Network Security Tools*, O'Reilly, 2005.		×		
7	*Security+™ A CompTIA Certification*, tài liệu kèm theo khóa học Security+.		×		
8	Harold F. Tipton, Micki Krause, *Information Security Management Handbook 5th*, CRC Press, 2004		×		
9	Bộ tài liệu ISO 27001		×		
10	Karen Mercedes Goertzel, *Software security assurance*, SOAR, 2007.		×		

7. Hình thức tổ chức dạy học

7.1. Lịch trình chung: (Ghi tổng số giờ cho mỗi cột)

Nội dung	Hình thức tổ chức dạy học học phần					Tổng
	Lên lớp			Thực hành, thí nghiệm, thực tập...	Tự học, tự ng.cứu	
	Lý thuyết	Bài tập	Thảo luận			
Chương 1. Tổng quan về an toàn	**3**					**3**

bảo mật hệ thống thông tin.						
Chương 2. Phân tích đánh giá nguy cơ về an toàn bảo mật hệ thông thông tin	**6**					**6**
Chương 3. Giải pháp an toàn bảo mật hệ thông thông tin	**15**					**15**
Chương 4. Quy chuẩn về an toàn bảo mật hệ thống	**3**					**3**
Chương 5. Đánh giá an toàn bảo mật hệ thống, dịch vụ an toàn hệ thống	**3**					**3**
Chủ đề 1: Xây giải pháp triển khai mã hóa cho cơ sở dữ liệu, truyền dữ liệu	**3**	**3**				**6**
Chủ đề 2: Phân tích lỗi của hệ thống phần mềm (mẫu), lỗi về ứng dụng, lỗi về web	**3**	**3**				**6**
Chủ đề 3: Xây dựng chức năng tấn công phần mềm, và kiểm tra tấn công phần mềm	**3**	**3**				**6**
Chủ đề 4: Xây dựng quy định về sử dụng ứng	**3**	**3**				**6**

dụng, và quy trình đảm bảo an toàn cho hệ thống (mẫu)						
Chủ đề 5: Mô hình tấn công hệ thống	**3**	**3**				**6**

7.2. Lịch trình tổ chức dạy học cụ thể

Bài giảng: Tổng quan về an toàn bảo mật hệ thống thông tin

Chương, mục: Chương I

Tiết thứ: 1-3 Tuần thứ: 1

Mục đích, yêu cầu:

Nắm được tổng quan về mục tiêu của an toàn và bảo mật hệ thống thông tin. Có nhìn nhận về 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 trong an toàn và bảo mật hệ thống thông tin.

- Hình thức tổ chức dạy học:

Giới thiệu lý thuyết

- Thời gian:

3 tiết

- Địa điểm:

Phòng học

- Nội dung chính:

Chương I: Vấn đề về an toàn và bảo mật hệ thống thông tin

- Thông tin
- Phạm vi hệ thống thông tin
- Đảm bảo và an toàn thông tin

1.2. Phạm vi vấn đề, một số nhìn nhận về an toàn bảo mật thông tin

- Phạm vi đảm bảo và an toàn thông tin

Một số khái niệm liên quan

1.3. Mục tiêu an toàn bảo mật hệ thống thông tin

- Mô hình tam giác mục tiêu
- Phân tích chi tiết các mục tiêu

Minh họa tương ứng mục tiêu và các vấn đề trong thực tiễn

1.4. Các khái niệm

1.5. Các nguồn nguy cơ với hệ thống thông tin

1.6. Các loại đe dọa với hệ thống thông tin

1.7. Quy trình quản lý nguy cơ

1.8. Giải pháp đảm bảo an toàn và bảo mật hệ thống thông tin

- Yêu cầu SV chuẩn bị:

Sinh viên tìm hiểu một số mô hình công nghệ thông tin, tìm các nguy cơ với một hệ thống thông tin.

- Ghi chú:

Đọc tài liệu tham khảo 1.

Bài giảng: Phân tích đánh giá nguy cơ về an toàn bảo mật hệ thông thông tin

Chương, mục: Chương II

Tiết thứ: 4-6 Tuần thứ: 2

Mục đích, yêu cầu:

Nắm được loại nguy cơ với hệ thống thông tin, yếu tố con người, yếu tố kỹ thuật. Các loại hình tấn công mạng máy tính thông dụng hiện tại.

- Hình thức tổ chức dạy học:

Giới thiệu lý thuyết

- Thời gian:

3 tiết

- Địa điểm:

Phòng học

- Nội dung chính:

2.1. Các nhóm nguy cơ và đánh giá

2.2. Những đe dọa từ nhân tố con người

Giới thiệu các đe dọa đến từ nhân tố con người: bỏ quyên, lỗi, trộm cắp, …

2.3. Những đe dọa đến từ nhân tố kỹ thuật

Tấn công mang tính kỹ thuật: tấn công mạng máy tính, tấn công mã độc

- Yêu cầu SV chuẩn bị:

Tìm hiểu các đe dọa với hệ thống thông tin.

- Ghi chú:

Đọc tài liệu tham khảo 1, 8.

Bài giảng: Phân tích đánh giá nguy cơ về an toàn bảo mật hệ thông thông tin

Chương, mục: Chương II

Tiết thứ: 7-9 Tuần thứ: 3

Mục đích, yêu cầu:

Các loại hình tấn công liên quan đến yếu tố con người. Các vấn đề về lỗi, và thiên tai, sự cố.

- Hình thức tổ chức dạy học:

Giới thiệu lý thuyết

- Thời gian:

3 tiết

- Địa điểm:

Phòng học

- Nội dung chính:

2.4. Kết hợp nhân tố con người và nhân tố kỹ thuật trong tấn công hệ thống

Tấn công social engeneering

2.5. Các đe dọa khác

– Lỗi thiết thiết bị

Các vấn đề tai họa, thiên tai

- Yêu cầu SV chuẩn bị:

Sinh viên tìm hiểu các thức tấn công xã hội. Các vấn đề về đảm bảo hệ thống trong các tình huống thiên tai, sự cố.

- Ghi chú:

Đọc tài liệu tham khảo 1, 8.

Bài giảng: Giải pháp an toàn bảo mật hệ thông thông tin

Chương, mục: Chương III

Tiết thứ: 10-12 Tuần thứ: 4

Mục đích, yêu cầu:

Sinh viên nắm được quan trọng của chính sách, tài liệu hướng dẫn liên quan đến an toàn bảo mật hệ thống thông tin.

- Hình thức tổ chức dạy học:

Giới thiệu lý thuyết

- Thời gian:

3 tiết

- Địa điểm:

Phòng học

- Nội dung chính:

3.1. Vấn đề an toàn bảo mật và chính sách

– Phân tích sự cần thiết phải có chính sách, tiêu chuẩn, chỉ dẫn và chương trình an toàn bảo mật hệ thống thông tin
– Một số chính sách tiêu biểu
– Kế hoạch công việc liên tục

Một số minh họa về chính sách phân lớp thông tin và quản lý tài liệu

- Yêu cầu SV chuẩn bị:

Sinh viên tìm hiểu các chính sách, tiêu chuẩn, quy định liên quan đến an toàn và bảo mật hệ thống thông tin.

- Ghi chú:

Đọc tài liệu tham khảo 1, 8.

Bài giảng: Giải pháp an toàn bảo mật hệ thông thông tin

Chương, mục: Chương III

Tiết thứ: 13-15 Tuần thứ: 5

Mục đích, yêu cầu:

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.

- Hình thức tổ chức dạy học:

Giới thiệu lý thuyết

- Thời gian:

3 tiết

- Địa điểm:

Phòng học

- Nội dung chính:

3.2. Vấn đề về an toàn bảo mật và mã hóa

– Sự quan trọng của mã hóa trong an toàn và bảo mật thông tin

Mô hình mã hóa thông tin, và đánh giá (mã hóa cổ điển, mã hóa tiêu chuẩn mới, mã hóa công khai, hàm băm)

- Yêu cầu SV chuẩn bị:

Sinh viên tìm hiểu các kỹ thuật liên quan đến mã hóa.

- Ghi chú:

Đọc tài liệu tham khảo 2.

Bài giảng: Giải pháp an toàn bảo mật hệ thông thông tin

Chương, mục: Chương III

Tiết thứ: 16-18 Tuần thứ: 6

Mục đích, yêu cầu:

Tìm hiểu các mô hình triển khai mã hóa, ứng dụng trong đảm bảo an toàn thông tin.

- Hình thức tổ chức dạy học:

Giới thiệu lý thuyết

- Thời gian:

3 tiết

- Địa điểm:

Phòng học

- Nội dung chính:

3.2. Vấn đề về an toàn bảo mật và mã hóa

– Mô hình triển khai mã hóa trong lưu trữ và truyền thông tin

Mô hình triển khai dịch vụ dựa trên mô hình mã hóa (chữ ký số, xác thực số, …)

- Yêu cầu SV chuẩn bị:

Sinh viên tìm hiểu các kỹ thuật liên quan đến mã hóa, triển khai trong thực tiễn.

- Ghi chú:

Đọc tài liệu tham khảo 2, 8.

Bài giảng: Giải pháp an toàn bảo mật hệ thông thông tin

Chương, mục: Chương III

Tiết thứ: 19-21 Tuần thứ: 7

Mục đích, yêu cầu:

Tìm hiểu các phần mềm, phần cứng, chuẩn đảm bảo an toàn bảo mật.

- Hình thức tổ chức dạy học:

Giới thiệu lý thuyết

- Thời gian:

3 tiết

- Địa điểm:

Phòng học

- Nội dung chính:

3.3. Vấn đề an toàn bảo mật và mạng máy tính

– Giải pháp chống tấn công mạng máy tính bằng thiết bị

– Giải pháp chống tấn công mạng máy tính bằng sử dụng phần mềm, chuẩn mới

Giải pháp chống mã độc

- Yêu cầu SV chuẩn bị:

Sinh viên tìm hiểu về các phần mềm, phần cứng, chuẩn đảm bảo an toàn bảo mật hệ thống.

- Ghi chú:

Đọc tài liệu tham khảo 6, 8.

Bài giảng: Giải pháp an toàn bảo mật hệ thông thông tin

Chương, mục: Chương III

Tiết thứ: 22-24 Tuần thứ: 8

Mục đích, yêu cầu:

Các lỗi trong lập trình, giải pháp để lập trình và phát triển ứng dụng an toàn trước tấn công vào ứng dụng.

- Hình thức tổ chức dạy học:

Giới thiệu lý thuyết

- Thời gian:

3 tiết

- Địa điểm:

Phòng học

- Nội dung chính:

3.4. Vấn đề an toàn bảo mật hệ thống thông tin trong phát triển phần mềm

– Một số vấn đề lỗi trong phát triển phần mềm

– Quy trình phát triển phần mềm an toàn

Một số vấn đề phát triển phần mềm an toàn

- Yêu cầu SV chuẩn bị:

Sinh viên tìm hiểu thông tin về lỗi tấn công phần mềm và giải pháp đảm bảo trong phát triển ứng dụng an toàn.

- Ghi chú:

Đọc tài liệu tham khảo 5, 10.

Bài giảng: Quy chuẩn về an toàn bảo mật hệ thống

Chương, mục: Chương IV

Tiết thứ: 25-27 Tuần thứ: 9

Mục đích, yêu cầu:

Hiểu mục tiêu, và cấu trúc của tiêu chuẩn ISO.

- Hình thức tổ chức dạy học:

Giới thiệu lý thuyết

- Thời gian:

3 tiết

- Địa điểm:

Phòng học

- Nội dung chính:

4.1. Giới thiệu về tiêu chuẩn an toàn và bảo mật cho hệ thống thông tin: ISO 27001, …

- Yêu cầu SV chuẩn bị:

Sinh viên tìm hiểu về tiêu chuẩn ISO 27001.

- Ghi chú:

Đọc tài liệu tham khảo 9.

Bài giảng: Đánh giá an toàn bảo mật hệ thống, dịch vụ an toàn hệ thống

Chương, mục: Chương V

Tiết thứ: 28-30 Tuần thứ: 10

Mục đích, yêu cầu:

Hiểu được các công cụ đánh giá an toàn bảo mật hệ thống. Các phương thức điều tra tội phạm về an toàn và bảo mật hệ thống thông tin.

- Hình thức tổ chức dạy học:

Giới thiệu lý thuyết

- Thời gian:

3 tiết

- Địa điểm:

Phòng học

- Nội dung chính:

5.1. Giới thiệu các công cụ đánh giá an toàn và bảo mật hệ thống thông tin

5.2. Giới thiệu các phương thức phát hiện tấn công

5.3. Phương thức điều tra tội phạm

- Yêu cầu SV chuẩn bị:

Sinh viên tìm hiểu các công cụ, phương pháp điều tra tội phạm.

- Ghi chú:

Đọc tài liệu tham khảo 6.

Bài giảng: Xây giải pháp triển khai mã hóa cho cơ sở dữ liệu, truyền dữ liệu

Chương, mục: Chủ đề nghiên cứu I

Tiết thứ: 31-36 Tuần thứ: 11-12

Mục đích, yêu cầu:

Hiểu được các đặc điểm của mã hóa, tìm hiểu mô hình hệ thống thông tin cụ thể. Phân tích đề xuất giải pháp và đánh giá.

- Hình thức tổ chức dạy học:

Giới thiệu lý thuyết

- Thời gian:

3 tiết

- Địa điểm:

Phòng học

- Nội dung chính:

- Sinh viên có mô hình về hệ thống, bao gồm cơ sở dữ liệu, các dịch vụ hoạt động
- Đánh giá mức độ quan trọng của dữ liệu hệ thống
- Lựa chọn phương thức mã hóa, dịch vụ mã hóa để đảm bảo cơ sở dữ liệu, các dịch vụ cung cấp của hệ thống an toàn
- Đề xuất giải pháp

Giới thiệu giải pháp, bình luận

- Yêu cầu SV chuẩn bị:

Sinh viên tìm hiểu mô hình, đề xuất giải pháp.

- Ghi chú:

Tổng hợp các kiến thức đã nghiên cứu.

Bài giảng: Phân tích lỗi của hệ thống phần mềm (mẫu), lỗi về ứng dụng, lỗi về web

Chương, mục: Chủ đề nghiên cứu II

Tiết thứ: 37-42 Tuần thứ: 13-14

Mục đích, yêu cầu:

Sinh viên tìm hiểu công cụ, khảo sát hệ thống ứng dụng mẫu, phân tích được lỗi tiềm ẩn trong ứng dụng.

- Hình thức tổ chức dạy học:

Giới thiệu lý thuyết

- Thời gian:

3 tiết

- Địa điểm:

Phòng học

- Nội dung chính:

- Sinh viên tiếp cận một trong hai mô hình phần mềm là ứng dụng trên desktop, và hệ thống web site
- Từ chương trình triển khai đánh giá sự tồn tại lỗi khả năng bị tấn công của hệ thống
- Từ mã nguồn đánh giá khả năng bị tấn công của hệ thống
- Giới thiệu giải pháp, bình luận

- Yêu cầu SV chuẩn bị:

Sinh viên tìm hiểu mô hình, thực hiện phân tích, đưa ra kết quả.

- Ghi chú:

Tổng hợp các kiến thức đã nghiên cứu.

Bài giảng: Xây dựng chức năng tấn công phần mềm, và kiểm tra tấn công phần mềm

Chương, mục: Chủ đề nghiên cứu III

Tiết thứ: 43-48 Tuần thứ: 15-16

Mục đích, yêu cầu:

Sinh viên thực hiện xây dựng minh họa về mã độc từ đó có kiến thức sâu hơn về cách thức tấn công mã độc từ đó có khả năng trong việc đảm bảo hệ thống trước tấn công mã độc.

- Hình thức tổ chức dạy học:

Giới thiệu lý thuyết

- Thời gian:

3 tiết

- Địa điểm:

Phòng học

- Nội dung chính:

- Xây dựng các mã có chức năng tương tự như mã độc
- Xây dựng ứng dụng phát hiện mã độc đã được xác định trước

– Giới thiệu chương trình, bình luận

- Yêu cầu SV chuẩn bị:

Sinh viên tìm hiểu mô hình, xây dựng các mã độc ví dụ minh họa.

- Ghi chú:

Tổng hợp các kiến thức đã nghiên cứu.

Bài giảng: Xây dựng quy định về sử dụng ứng dụng, và quy trình đảm bảo an toàn cho hệ thống

Chương, mục: Chủ đề nghiên cứu IV

Tiết thứ: 49-54 Tuần thứ: 17-18

Mục đích, yêu cầu:

Sinh viên tổng hợp kiến thức đề xuất giải pháp an toàn bảo mật cho một hệ thống thực tế.

- Hình thức tổ chức dạy học:

Giới thiệu lý thuyết

- Thời gian:

3 tiết

- Địa điểm:

Phòng học

- Nội dung chính:

– Yêu cầu sinh viên đề ra các yêu cầu để đảm bảo an toàn bảo mật hệ thống thông tin cho cho việc phát triển một hệ thống (từ bảo mật cơ sở dữ liệu, truyền dữ liệu, phân quyền, quy định sử dụng phần mềm, chính sách về backup, các kế hoạch công việc liên tục tương ứng với hệ thống)

Giới thiệu, bình luận

- Yêu cầu SV chuẩn bị:

Sinh viên tìm hiểu mô hình. Đề xuất giải pháp.

- Ghi chú:

Tổng hợp các kiến thức đã nghiên cứu.

Bài giảng: Mô hình tấn công hệ thống

Chương, mục: Chủ đề nghiên cứu V

Tiết thứ: 55-60 Tuần thứ: 19-20

Mục đích, yêu cầu:

Tìm hiểu mô hình hệ thống thực tế đề tìm điểm yếu đề xuất các giải pháp để tấn công hệ thống.

- Hình thức tổ chức dạy học:

Giới thiệu lý thuyết

- Thời gian:

3 tiết

- Địa điểm:

Phòng học

- Nội dung chính:

- Cho một hệ thống thực tế, tấn công hệ thống với công cụ, kiến thức có được, phát triển công cụ, hoặc mở rộng các công cụ, phương thức tấn công mới với hệ thống.

- Đưa ra các bước tiếp cận, phân tích

- Yêu cầu SV chuẩn bị:

Sinh viên tìm hiểu mô hình. Đề xuất giải pháp.

- Ghi chú:

Tổng hợp các kiến thức đã nghiên cứu.

8. Chính sách đối với học phần và các yêu cầu khác của giáo viên

Sinh viên tham gia đầy đủ các buổi học trên lớp theo quy định của phòng đào tạo. Tham gia bài kiểm tra đánh giá giữa kỳ.

9. Phương pháp, hình thức kiểm tra - đánh giá kết quả học tập học phần

9.1. Kiểm tra – đánh giá thường xuyên:

Thường xuyên điểm danh vào thời điểm thích hợp

9.2. Kiểm tra - đánh giá định kì:

- Tham gia học tập trên lớp (đi học đầy đủ, chuẩn bị bài tốt và tích cực thảo luận,…): *hệ số 0.10.*
- Hoàn thành tốt Bài tập về nhà , Kiểm tra giữa kì : *hệ số 0.2*
- Thi kết thúc học phần tốt: *hệ số 0.7*

Chủ nhiệm Khoa	**Chủ nhiệm Bộ môn**	**Giảng viên biên soạn**
(Ký và ghi rõ họ tên)	*(Ký và ghi rõ họ tên)*	*(Ký và ghi rõ họ tên)*