TRƯỜNG ĐH TÀI CHÍNH - NGÂN HÀNG HÀ NỘI
KHOA CÔNG NGHỆ THÔNG TIN
BỘ MÔN TIN ỨNG DỤNG

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

Hệ đào tạo: Đại học chính quy
Ngành: Công nghệ thông tin, chuyên ngành Tin ứng dụng

1. Thông tin chung về học phần

- **Tên học phần: AN TOÀN VÀ BẢO MẬT THÔNG TIN**
  (Safety and Security Information)
- **Mã học phần: DCT.02.21**
- **Số tín chỉ: 3**
- **Phân bổ giờ tín chỉ đối với các hoạt động: (số lượng tiết)**
  + Lý thuyết và thực hành: 27 tiết
  + Bài tập lớn, thảo luận, kiểm tra: 30 tiết
  + Kiểm tra: 3 tiết.
- **Khoa, Bộ môn phụ trách học phần**: Bộ môn Tin ứng dụng Khoa CNTT
- **Giảng viên phụ trách học phần (dự kiến):**
  1) Họ và tên: TS. Bùi Đức Tiến
  Chức danh: Giảng viên cao cấp
  Thông tin liên hệ: ĐT: 0913514311; Email: tienbuiduc@gmail.com

2. Các học phần tiên quyết

Các học phần tiên quyết:

- Quản trị mạng (Mã số DCT.02.13**)**

3. Mục tiêu của học phần:

3.1 Mục tiêu chung:

Môn học cung cấp cho sinh viên các khái niệm và nguyên tắc cơ bản về đảm bảo an toàn thông tin.

3.2 Mục tiêu cụ thể

a) Về kiến thức: Trang bị cho sinh viên kiến thức chung về an toàn và bảo mật thông tin.

b) Về kỹ năng: Biết tổ chức thực hiện an toàn và bảo mật thông tin cho một hệ thống. Biết sử dụng một số công cụ đảm bảo ATTT.

c) Về thái độ: Giúp sinh viên nhận thức được tầm quan trọng của ANTT; vai trò, trách nhiệm và đạo đức của người làm công việc an toàn vào bảo mật thông tin: cẩn thận, làm việc theo đúng quy trình, có tinh thần trách nhiệm và đạo đức nghề nghiệp.

4. Chuẩn đầu ra của học phần

4.1. Nội dung chuẩn đầu ra học phần:

1) Về kiến thức:

CLO 1: Nhận thức được tầm quan trọng của ATBMTT. Hiểu được các kiến thức về ATBMTT

CLO 2: Vận dụng được các kiến thức về ATBMTT để nhận biết được các dấu hiệu mất an toàn, bảo mật thông tin của một hệ thống và các phương pháp phòng chống, xử lý. Thiết kế được các hệ thống đảm bảo ATTT.

CLO 3: Phân tích, đánh giá được các giải pháp ATBMTT.

2) Về kỹ năng

CLO 4: Thiết kế được các hệ thống an toàn và bảo mật cho doanh nghiệp.

CLO 5: Đánh giá các bản thiết kế về ATBMTT cho các hệ thống thông tin.

CLO 6: Có thể sử dụng một số công cụ đảm bảo ATBMTT.

3) Về phẩm chất

CLO 7: Có phẩm chất chính trị; có trách nhiệm công dân, trách nhiệm cộng đồng. Có đạo đức nghề nghiệp, có tinh thần hợp tác và thái độ phục vụ tốt. Năng động, có hoài bão về nghề nghiệp.

Ghi chú: CLO = Course Learning Outcomes = Chuẩn đầu ra của học phần.

4.2. Ma trận nhất quán giữa chuẩn đầu ra học phần (CLO) với chuẩn đầu ra chương trình đào tạo (PLO):

	PLO 1	PLO 2	PLO 3	PLO 4	PLO 5	PLO 6	PLO 7	PLO 8	PLO 9
CLO 1				H	H	M	M	M	M
CLO 2				H	H	M	M	M	M
CLO 3				H	H	M	M	M	M
CLO 4				H	M	H	H	H	M
CLO 5				H	M	H	H	H	M
CLO 6				H	M	H	H	H	M
CLO 7				M	M	H	H	H	H
Tổng hợp toàn bộ học phần				H	M	H	H	H	M

Ghi chú:

- PLO = Program Learning Outcomes = Chuẩn đầu ra của chương trình đào tạo

- Mức độ đóng góp của CLO và PLO được xác định cụ thể như sau:

L (Low) – CLO có đóng góp ít vào PLO

M (Medium) – CLO có đóng góp vừa vào PLO

H (High) - CLO có đóng góp nhiều vào PLO

Chú thích: H – cao; M – vừa; L – thấp – phụ thuộc vào mức hỗ trợ của CLO đối với PLO ở mức bắt đầu (L) hoặc mức nâng cao hơn mức bắt đầu; có nhiều cơ hội được thực hành, thí nghiệm, thực tế (mức M) hay mức thuần thục, thành thạo (H)).

4.3. Ma trận nhất quán giữa phương pháp, hình thức kiểm tra, đánh giá với chuẩn đầu ra học phần (CLO)

Ghi chú: *Khi xây dựng bảng này, xem mục 5.1 để về các hình thức kiểm tra, đánh giá mà giảng viên sử dụng khi giảng dạy học phần*

Hình thức đánh giá	CLO1	CLO2	CLO3	CLO4	CLO5	CLO6	CLO7
1. Chuyên cần	H	H	H	M	M	M	M
2. Vấn đáp/BTL	H	H	H	H	H	H	H
3. Viết	H	H	H	M	M	M	M
4. Thực hành							

4.4. Ma trận nhất quán giữa phương pháp dạy học với chuẩn đầu ra học phần (CLO)

Phương pháp giảng dạy	CLO1	CLO2	CLO3	CLO4	CLO5	CLO6	CLO7
1. Thuyết trình (Trực tiếp, Online)	M	M	M	M	M	M	M
2. Dạy & học thực hành	H	H	H	H	H	H	M
3. Hướng dẫn tự học	M	M	M	M	M	M	M

4.5. Ma trận nhất quán các chương với chuẩn đầu ra học phần (CLO)

Chú thích*:* **I**: Introduction/ Giới thiệu

P: Proficient/ Thuần thục, đủ

A: Advanced/ Nâng cao

	CLO 1	CLO 2	CLO 3	CLO 4	CLO 5	CLO 6	CLO 7
Bài 1	I	I	I	I	I	I	I
Bài 2-5	A	A	A	P	P	P	P
Bài 6-9	A	A	A	A	A	A	P
Bài 10-13	A	A	A	P	P	P	P
Bài 14-17	A	A	A	A	A	A	P
Bài 18-20	A	A	A	P	P	P	A

(Xem chi tiết tiêu đề các bài ở Mục 8)

5. Nhiệm vụ của sinh viên

- Tham dự giờ lên lớp: tối thiểu 80% số tiết học trên lớp, trong phòng thực hành có sự giảng dạy, hướng dẫn trực tiếp của giáo viên;
- Bài tập, thảo luận:
  + Đọc tài liệu, chuẩn bị và tham gia thảo luận theo hướng dẫn của giáo viên;
  + Thực hiện đầy đủ các bài tập được giao;
- Làm bài kiểm tra định kỳ;
- Tham gia thi kết thúc học phần.

6. Tài liệu học tập:

6.1. Giáo trình chính:

[1]. Hoàng Xuân Dậu, Nguyễn Thị Thanh Thủy (2016), *Bài giảng cơ sở an toàn thông tin,* ĐH Bưu chính viễn thông.

6.2. Sách tham khảo:

[1]. ĐH Kinh doanh và Công nghệ HN (2013), Giáo trình Bảo mật thông tin

7. Mô tả vắn tắt nội dung học phần:

Học phần gồm các nội dung chính sau:

Chương 1- Tổng quan về an toàn thông tin. Giới thiệu các khái niệm về an toàn thông tin (ATTT), an toàn hệ thống thông tin (HTTT) và các yêu cầu đảm bảo an toàn thông tin, an toàn hệ thống thông tin. Chương cũng đề cập các nguy cơ, rủi ro trong các vùng của hạ tầng công nghệ thông tin theo mức kết nối mạng. Phần cuối của chương giới thiệu mô hình tổng quát đảm bảo an toàn thông tin, an toàn hệ thống thông tin.

Chương 2- Các lỗ hổng bảo mật và các điểm yếu hệ thống. Giới thiệu các khái niệm về các điểm yếu và lỗ hổng bảo mật tồn tại trong hệ thống, các dạng lỗ hổng bảo mật trong hệ điều hành và các phần mềm ứng dụng. Chương đi sâu phân tích cơ chế xuất hiện và khai thác các lỗ hổng tràn bộ đệm và lỗ hổng không kiểm tra đầu vào. Phần cuối của chương đề cập vấn đề quản lý, khắc phục các lỗ hổng bảo mật, tăng cường khả năng đề kháng cho hệ thống và giới thiệu một số công cụ rà quét lỗ hổng bảo mật.

Chương 3- Các dạng tấn công và các phần mềm độc hại. Giới thiệu về các dạng tấn công điển hình vào các hệ thống máy tính và mạng, bao gồm tấn công vào mật khẩu, tấn công nghe lén, người đứng giữa, tấn công DoS, DDoS, tấn công sử dụng các kỹ thuật xã hội,… Nửa cuối của chương đề cập đến các dạng phần mềm độc hại, gồm cơ chế lây nhiễm và tác hại của chúng. Kèm theo phần mô tả mỗi tấn công, hoặc phần mềm độc hại, chương đề cập các biện pháp, kỹ thuật phòng chống.

Chương 4 – Đảm bảo an toàn thông tin dựa trên mã hóa. Giới thiệu các khái niệm cơ bản về mật mã, hệ mã hóa, các phương pháp mã hóa. Phần tiếp theo của chương trình bày một số giải thuật cơ bản của mã hóa khóa đối xứng (DES, 3-DES và AES), mã hóa khóa bất đối xứng (RSA) và các hàm băm (MD5 và SHA1).

Chương 5- Các kỹ thuật và công nghệ đảm bảo an toàn thông tin giới thiệu khái quát về điều khiển truy nhập, các cơ chế (mô hình) điều khiển truy nhập và một số công nghệ điều khiển truy nhập được sử dụng trên thực tế. Phần tiếp theo của chương giới thiệu về tường lửa – một trong các kỹ thuật đoợc sử dụng rất phổ biến trong đảm bảo an toàn cho hệ thống máy tính và mạng. Phần cuối của chương giới thiệu về các hệ thống phát hiện và ngăn chặn xâm nhập và các công cụ rà quét phần mềm độc hại.

Chương 6 – Quản lý, chính sách và pháp luật an toàn thông tin. Giới thiệu một số khái niệm cơ bản trong quản lý an toàn thông tin, vấn đề đánh giá rủi ro an toàn thông tin và thực thi quản lý an toàn thông tin. Nội dung tiếp theo được đề cập là các chuẩn quản lý an toàn thông tin, trong đó giới thiệu một số chuẩn của bộ chuẩn ISO/IEC 27000. Phần cuối của chương giới thiệu khái quát về các vấn đề chính sách, pháp luật và đạo đức an toàn thông tin.

8. Kế hoạch giảng dạy:

Bài dạy	**Nội dung giảng dạy**	**Số tiết** (LT, BT, TH)	**Nhiệm vụ của sinh viên**

Bài dạy	Nội dung giảng dạy	Số tiết (LT, BT, TH)	Nhiệm vụ của sinh viên
Bài 1	Chương 1. Tổng quan về an toàn thông tin (ATTT). 1.1. Khái quát về ATTT 1.2. Các yêu cầu đảm bảo ATTT và HTTT 1.3. Các thành phần của ATTT 1.4. Các mối đe dọa và nguy cơ trong các vùng hạ tầng CNTT 1.5. Mô hình tổng quát đảm bảo ATTT và HTTT	3 LT	Đọc trước giáo trình, làm bài tập cuối chương
Bài 2+3+4	Chương 2. Các lỗ hổng bảo mật và điểm yếu hệ thống. 2.1. Tổng quan về lỗ hổng bảo mật và các điểm yếu hệ thống 2.2. Các dạng lỗ hổng trong hệ điều hành và phần mềm ứng dụng. 2.3. Quản lý, khắc phục các lỗ hổng bảo mật và tăng cường khả năng đề kháng cho hệ thống 2.4. Giới thiệu một số công cụ rà quét điểm yếu và lỗ hổng bảo mật (SV tự nghiên cứu)	6 tiết LT 3 tiết SV tự nghiên cứu	Đọc trước giáo trình, làm bài tập cuối chương
Bài 5	Thảo luận chương 1+2	3	Chuẩn bị câu hỏi
Bài 6+7+8	Chương 3: Các dạng tấn công và các phần mềm độc hại 3.1. Khái quát về mối đe dọa và tấn công 3.2. Các công cụ hỗ trợ tấn công 3.3. Các dạng tấn công thường gặp 3.4. Các dạng phần mềm độc hại (SV tự học)	6 tiết LT 3 tiết tự học	Đọc trước giáo trình, làm bài tập cuối chương
Bài 9	Thảo luận chương 3 Kiểm tra giữa kì lần 1	2 tiết 1 tiết KT	Chuẩn bị câu hỏi, làm bài KT
Bài 10+11 +12 +13	Chương 4 – Đảm bảo an toàn thông tin dựa trên mã hóa 4.1. Khái quát về mã hóa thông tin và ứng dụng 4.2. Các phương pháp mã hóa 4.3. Các giải thuật mã hóa 4.4. Các hàm băm (SV tự học)	6 LT 6 tự học	Đọc trước giáo trình, làm bài tập cuối chương
Bài 14+15 +16	Chương 5- Các kỹ thuật và công nghệ đảm bảo an toàn thông tin 5.1. Điều khiển truy nhập	6 LT 3 tiết tự nghiên cứu	Đọc trước giáo trình, làm bài tập cuối chương

Bài dạy	Nội dung giảng dạy	Số tiết (LT, BT, TH)	Nhiệm vụ của sinh viên
	5.2. Tường lửa 5.3. Các hệ thống phát hiện và ngăn chặn xâm nhập 5.4. Các công cụ rà quét phần mềm độc hại		
Bài 17	Thảo luận chương 4+5 Kiểm tra giữa kì lần 2	2 TH 1 tiết KT	Chuẩn bị câu hỏi, làm bài KT
Bài 18 +19	Chương 6 – Quản lý, chính sách và pháp luật an toàn thông tin 6.1. Quản lý an toàn thông tin 6.2. Các chuẩn quản lý an toàn thông tin 6.3. Pháp luật và chính sách ATTT 6.4. Vấn đề đạo đức ATTT	3 tiết LT 3 tiết tự nghiên cứu	Đọc trước giáo trình, làm bài tập cuối chương
Bài 20	Thảo luận chương 6 và toàn bộ học phần	3 tiết	Chuẩn bị câu hỏi

9. Cơ sở vật chất phục vụ giảng dạy:

- Tên giảng đường:
- Danh mục trang thiết bị: Projector, mạng có thể truy nhập Internet

10. Kiểm tra, đánh giá kết quả học tập:

10.1. Phương pháp, hình thức kiểm tra, đánh giá

10.1.1 Kiểm tra – đánh giá thường xuyên: Trên lớp (Lấy điểm chuyên cần)

STT	Hình thức đánh giá	Trọng số	Yêu cầu chung, mục đích, minh chứng
1.	Điểm chuyên cần: Đánh giá mức độ thực hiện các nhiệm vụ sinh viên, bao gồm việc tham gia học tập trên lớp và kiểm tra, đánh giá thường xuyên trên lớp	10%	+ Mục đích: Giúp sinh viên duy trì ý thức, kỷ luật trong học tập. + Yêu cầu: ▪ Sinh viên đi học đều đặn, đúng giờ. ▪ Sinh viên thực hiện đầy đủ các yêu cầu chuẩn bị học tập của GV.

10.1.2. Kiểm tra - đánh giá định kỳ, thi kết thúc học phần

STT	Hình thức đánh giá	Trọng số	Yêu cầu chung, mục đích, minh chứng
1.	03 điểm đánh giá giữa kỳ: làm bài	30%	+ Mục đích: Giúp sinh viên củng cố

	tự luận/ trắc nghiệm		kiến thức đã được học. + Yêu cầu: Sinh viên làm bài độc lập
2.	Kiểm tra cuối kỳ: tự luận/ trắc nghiệm	60%	+ Mục đích: Đánh giá kết quả học tập toàn bộ học phần của SV. + Yêu cầu: Sinh viên làm bài độc lập.

10.2. Miêu tả chi tiết các bài kiểm tra trong kỳ, bài thi hết học phần và bộ tiêu chí đánh giá:

- Bài kiểm tra trong kỳ, bài thi hết học phần: sinh viên làm bài tự luận/ trắc nghiệm độc lập

- Mô tả chi tiết:

(1) Bài kiểm tra giữa kỳ lần 1 phải có các câu hỏi trải đều trong 3 chương đầu. Trrong đó phải có các câu hỏi về các vấn đề: yêu cầu đảm bảo ATTT, thành phần của ATTT, các mối đe dọa và nguy cơ trong các vùng hạ tầng thông tin, mô hình tổng quát đảm bảo ATTT, các lỗ hổng và điểm yếu hệ thống; quản lý, khắc phục các lỗ hổng bảo mật; công cụ rà quét điểm yếu, lỗ hổng bảo mật thông dụng; các dạng tấn công và phần mềm độc hại.

(2) Bài kiểm tra giữa kỳ lần 2 phải có các câu hỏi trải đều trong chương 4 và 5. Trong đó phải có các câu hỏi về các vấn đề: mã hóa thông tin, các kỹ thuật và công nghệ đảm bảo ATTT.

(3) Bài liểm tra hết học phần phải có các câu hỏi trải đều trong toàn bộ học phần.

❖ **Tiêu chí đánh giá bài kiểm tra, bài thi kết thúc học phần**

Tiêu chí đánh giá	Mức chất lượng	Thang điểm
– Nội dung đủ, trả lời đúng 100% câu hỏi. – Trình bày rõ ràng, diễn đạt ngắn gọn, súc tích, logic. – Không có lỗi về thuật ngữ chuyên môn. – Không có lỗi chính tả.	Xuất sắc	9-10
– Trả lời đúng 70-80% câu hỏi. – Trình bày rõ ràng, diễn đạt logic. – Mắc ít lỗi (1-2 lỗi) về thuật ngữ chuyên môn. – Còn lỗi chính tả.	Khá- Giỏi	7-8
– Trả lời đúng 50-60% câu hỏi. – Trình bày không rõ ý, chưa logic. – Mắc lỗi về thuật ngữ chuyên môn (3-4 lỗi). – Còn lỗi chính tả.	Trung bình	5-6
– Trả lời sai, lạc đề, hoặc phần trả lời đúng dưới mức 50% câu hỏi. – Không làm hết câu hỏi, bỏ nội dung hơn 50%. – Trình bày tối nghĩa, diễn đạt không rõ ý.	Yếu	3-4

– Mắc nhiều lỗi về thuật ngữ chuyên môn (5-6 lỗi). – Nhiều lỗi chính tả.		
– Trả lời sai, lạc đề, phần trả lời đúng dưới mức 20%. – Không làm hết câu hỏi, bỏ đến 80% nội dung. – Trình bày tối nghĩa, diễn đạt không rõ ý. – Nhiều lỗi chính tả.	Kém	0-2

10.3. Chính sách trong đánh giá chuyên cần:

- Sinh viên vắng mặt quá 20% số buổi sẽ không được làm bài thi kết thúc học phần.

- Có điểm thưởng cho sinh viên tích cực phát biểu, ham học hỏi, có sự sáng tạo trong thảo luận, tranh biện.

Hà Nội, ngày 31 tháng 10 năm 2019

Hiệu trưởng	**Trưởng Khoa**	**Trưởng bộ môn**	**Người soạn đề cương**
PGS.TS. Phạm Ngọc Ánh	TS. Phùng Văn Ổn	ThS. Vũ Minh Tâm	TS. Bùi Đức Tiến