BỘ KHOA HỌC VÀ CÔNG NGHỆ
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Số: 541 /QĐ-HV

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

Hà Nội, ngày 13 tháng 03 năm 2026

QUYẾT ĐỊNH
Ban hành Chương trình đào tạo ngành An toàn thông tin trình độ thạc sĩ

GIÁM ĐỐC HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Căn cứ Quyết định số 171/QĐ-BKHCN ngày 03 tháng 3 năm 2025 ban hành Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Học viện Công nghệ Bưu chính Viễn thông;

Căn cứ Nghị quyết số 22/NQ-HĐHV ngày 12 tháng 4 năm 2021 của Hội đồng học viện về việc ban hành Quy chế tổ chức và hoạt động của Học viện Công nghệ Bưu chính Viễn thông và Nghị quyết số 191/NQ-HĐHV ngày 12/4/2025 về Điều chỉnh Quy chế tổ chức và hoạt động của Học viện Công nghệ Bưu chính Viễn thông;

Căn cứ Thông tư số 17/2021/TT-BGDĐT ngày 22 tháng 6 năm 2021 của Bộ trưởng Bộ Giáo dục và Đào tạo ban hành Quy định về chuẩn chương trình đào tạo; xây dựng, thẩm định, ban hành chương trình đào tạo các trình độ của giáo dục đại học;

Căn cứ Quyết định số 977/QĐ-HV ngày 13 tháng 6 năm 2025 của Giám đốc Học viện Công nghệ Bưu chính Viễn thông ban hành Quy định xây dựng, cải tiến và phát triển chương trình đào tạo;

Xét đề nghị của Trưởng phòng Đào tạo và Trưởng khoa An toàn thông tin,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này **Chương trình đại học ngành An toàn thông tin** trình độ thạc sĩ của Học viện Công nghệ Bưu chính Viễn thông *(Chi tiết kèm theo)*.

Điều 2. Quyết định có hiệu lực thi hành kể từ ngày ký.

Điều 3. Phó Giám đốc Phụ trách Cơ sở Học viện tại Tp. Hồ Chí Minh, Chánh văn phòng, Trưởng các Phòng: Đào tạo, Giáo vụ, Chính trị & Công tác sinh viên, Tài chính kế toán, Quản lý Khoa học công nghệ & hợp tác quốc tế; Trưởng Trung tâm Khảo thí & Đảm bảo chất lượng giáo dục, Trưởng các Khoa đào tạo 1 và 2, Trưởng Bộ môn Marketing, Trưởng khoa đào tạo sau đại học và Trưởng các đơn vị có liên quan chịu trách nhiệm thi hành Quyết định./.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

PGS.TS Trần Quang Anh

Nơi nhận:
- Như Điều 3;
- Bộ GD&ĐT *(để b/c)*;
- Bộ KH&CN *(để b/c)*;
- Ban Giám đốc HV;
- Lưu VT, ĐT (03).

BỘ KHOA HỌC VÀ CÔNG NGHỆ
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

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

CHƯƠNG TRÌNH ĐÀO TẠO

Ngành đào tạo (tiếng Việt):	**An toàn thông tin**
Ngành đào tạo (tiếng Anh):	**Information Security**
Trình độ đào tạo:	**Thạc sĩ**
Mã số:	**8480202**
Hình thức đào tạo:	**Chính quy**

(Kèm theo Quyết định số 541/QĐ-HV ngày 13 tháng 3 năm 2026 của Giám đốc Học viện)

1. MỤC TIÊU

1.1. Mục tiêu chung

Chương trình đào tạo thạc sĩ ngành An toàn thông tin của Học viện Công nghệ Bưu chính Viễn thông được thiết kế nhằm đào tạo người học có phẩm chất chính trị, đạo đức; có kiến thức, kỹ năng thực hành nghề nghiệp, năng lực nghiên cứu và ứng dụng kỹ thuật, công nghệ tương xứng với trình độ đào tạo bậc thạc sĩ; có khả năng học tập suốt đời; có khả năng sáng tạo và thích nghi với môi trường làm việc đa ngành; có ý thức trách nhiệm nghề nghiệp, đáp ứng yêu cầu phát triển kinh tế, xã hội và hội nhập quốc tế.

1.2 Mục tiêu cụ thể

Mục tiêu cụ thể của chương trình đào tạo thạc sĩ ngành An toàn thông tin của Học viện Công nghệ Bưu chính Viễn thông nhằm đào tạo thạc sĩ An toàn thông tin có:

PO1. Khả năng áp dụng kiến thức và kỹ năng của mình để đạt được thành công trong sự nghiệp và/hoặc theo học tập ở bậc sau đại học để lấy bằng tiến sĩ, hoặc các bằng cấp khác cao hơn;

PO2. Khả năng tư duy, giải quyết vấn đề một cách sáng tạo, giao tiếp hiệu quả và hoạt động thành công trong các nhóm đa ngành đa dạng và toàn diện;

PO3. Khả năng cư xử có đạo đức và trách nhiệm, sẽ luôn được cập nhật thông tin thông qua giáo dục liên tục và sẽ tham gia đầy đủ vào các hoạt động nghề nghiệp và xã hội;

PO4. Khả năng áp dụng các lý thuyết và kỹ thuật, công nghệ và quản lý bảo mật hiện đại và phù hợp để bảo vệ hạ tầng máy tính, mạng, dữ liệu, quy trình và người dùng khỏi các nguy cơ, các dạng tấn công, xâm nhập.

2. CHUẨN ĐẦU RA CỦA CHƯƠNG TRÌNH ĐÀO TẠO (PLOs)

Các chuẩn đầu ra (Learning Outcomes – PLOs) và các chỉ báo (Performance Indicator - PI) của chương trình đào tạo là thước đo mức kiến thức và kỹ năng tối thiểu mà người học

cần đạt được khi tốt nghiệp. Các PLO và PI kèm theo được thiết kế theo chuẩn kiểm định quốc tế ASIIN, với mức mức kiến thức và kỹ năng tương đương bậc 7 trong Khung trình độ quốc gia Việt Nam. Cụ thể, các PLO và PI của chương trình đào tạo cho như bảng sau:

Chuẩn đầu ra (PLOs)	Mức độ năng lực*	Các chỉ báo (PIs)
PLO1. Phân tích một bài toán phức tạp và áp dụng các kiến thức tính toán liên ngành để xác định các giải pháp giải quyết bài toán.	C4/P3	*PI1.1. Phát biểu bài toán và các yêu cầu.* *PI1.2. Phân tích các giải pháp tính toán để giải quyết bài toán.* *PI1.3. Lựa chọn giải pháp phù hợp dựa trên các nguyên lý tính toán để giải quyết bài toán.*
PLO2. Giao tiếp hiệu quả trong nhiều bối cảnh bối cảnh khoa học và chuyên môn.	C4/P3	*PI2.1. Thể hiện kỹ năng giao tiếp bằng văn bản hiệu quả trong nhiều bối cảnh bối cảnh khoa học và chuyên môn.* *PI2.2. Trình bày các vấn đề một cách hiệu quả sử dụng bài thuyết trình miệng trong nhiều bối cảnh bối cảnh khoa học và chuyên môn.*
PLO3. Nhận thức được trách nhiệm nghề nghiệp và đưa ra những đánh giá sáng suốt trong hoạt động bảo mật dựa trên các nguyên tắc pháp lý và đạo đức.	C4/P3/A3	*PI3.1. Áp dụng các nguyên tắc pháp lý và đạo đức nghề nghiệp khi giải quyết các vấn đề có liên quan đến nghề nghiệp.* *PI3.2.Thể hiện nhận thức về tầm quan trọng của sự riêng tư và bảo mật trong quản lý hệ thống và dữ liệu.*
PLO4. Hoạt động hiệu quả với tư cách là thành viên hoặc lãnh đạo một nhóm tham gia vào các hoạt động phù hợp với chuyên môn.	P3/A3	*PI4.1. Phối hợp, chia sẻ công việc trong một nhóm chuyên môn.* *PI4.2. Hoàn thành nhiệm vụ trong các vai trò khác nhau của nhóm chuyên môn.*
PLO5. Thiết kế, triển khai và đánh giá giải pháp bảo mật cho hệ thống đáp ứng một tập hợp các yêu cầu xác định.	C6/P4	*PI5.1. Đề xuất, thiết kế mô hình/giải pháp bảo mật hệ thống theo một tập các yêu cầu xác định.* *PI5.2. Triển khai mô hình/giải pháp bảo mật đã thiết kế.* *PI5.3. Đánh mô hình/giải pháp bảo mật đã triển khai.*

(C: miền kiến thức; P: miền kỹ năng; A: miền thái độ; Các mức độ năng lực được xác định trên cơ sở tham chiếu Thang cấp độ tư duy Bloom)

3. KHỐI LƯỢNG KIẾN THỨC TOÀN KHÓA:

Khối lượng kiến thức toàn khoá là **60 tín chỉ**.

4. ĐỐI TƯỢNG TUYỂN SINH VÀ YÊU CẦU ĐẦU VÀO

4.1 Đối tượng tuyển sinh:

- Là người đã tốt nghiệp trình độ đại học các ngành phù hợp theo quy định của Học viện Công nghệ Bưu chính Viễn thông. Đối với chương trình định hướng nghiên cứu, yêu cầu hạng tốt nghiệp trình độ đại học từ Khá trở lên hoặc có công trình khoa học liên quan đến lĩnh vực học tập, nghiên cứu;

- Có năng lực tiếng Anh từ bậc 3 trở lên theo Khung năng lực ngoại ngữ 6 bậc dùng cho Việt Nam hoặc tương đương theo Quy định tuyển sinh và đào tạo trình độ thạc sĩ của Học viện Công nghệ Bưu chính Viễn thông;

- Các điều kiện khác theo quy định tại Quy định tuyển sinh và đào tạo trình độ thạc sĩ của Học viện Công nghệ Bưu chính Viễn thông.

4.2 Yêu cầu đầu vào: Đã tham dự kỳ tuyển sinh cao học của Học viện Công nghệ Bưu chính Viễn thông và đủ điều kiện xét trúng tuyển trong kỳ tuyển sinh.

5. QUY TRÌNH ĐÀO TẠO, ĐIỀU KIỆN TỐT NGHIỆP

5.1. Quy trình đào tạo

Chương trình đào tạo được thực hiện trong 1,5 năm gồm 4 học kỳ, trong đó 3 học kỳ tích lũy kiến thức tại Học viện và 1 kỳ tốt nghiệp. Với chương trình thạc sĩ định hướng ứng dụng, kỳ tốt nghiệp bao gồm thực tập tốt nghiệp tại tổ chức, doanh nghiệp và làm đề án tốt nghiệp. Với chương trình thạc sĩ định hướng nghiên cứu, kỳ tốt nghiệp chỉ bao gồm luận văn tốt nghiệp.

Học viên được đào tạo theo phương thức đào tạo tín chỉ, áp dụng Quy chế đào tạo tín chỉ hiện hành của Bộ Giáo dục & Đào tạo và của Học viện.

5.2. Công nhận tốt nghiệp

a) Yêu cầu để được công nhận tốt nghiệp:

- Đã hoàn thành các học phần của chương trình đào tạo đạt yêu cầu từ 5,5 (theo thang điểm 10) trở lên;

- Bảo vệ thành công luận văn/đề án, đạt điểm từ 5,5 (theo thang điểm 10) trở lên;

- Có trình độ tiếng Anh đạt từ bậc 4 trở lên theo Khung năng lực ngoại ngữ 6 bậc dùng cho Việt Nam hoặc tương đương theo Quy định tuyển sinh và đào tạo trình độ thạc sĩ của Học viện Công nghệ Bưu chính Viễn thông;

- Chấp hành đúng các quy chế, quy định hiện hành của Bộ GD&ĐT và của Học viện Công nghệ Bưu chính Viễn thông.

b) Kết thúc khóa học, học viên được công nhận tốt nghiệp và được cấp bằng **Thạc sĩ ngành An toàn thông tin** hệ chính quy khi đã hội tụ đủ các tiêu chuẩn theo quy chế đào tạo trình độ thạc sĩ.

6. THANG ĐIỂM

Thực hiện theo thang điểm tín chỉ, trong đó điểm chữ (A, B, C, D, F) và thang điểm 4 quy đổi tương ứng được sử dụng để đánh giá kết quả học tập chính thức. Thang điểm 10 được sử dụng để đánh giá điểm thành phần của các học phần.

	Thang điểm 10 *(điểm thành phần)*	Thang điểm 4	
		Điểm chữ	Điểm số
Điểm đạt	Từ 9,0 đến 10,0	A+	4,0
	Từ 8,5 đến 8,9	A	3,7
	Từ 8,0 đến 8,4	B+	3,5
	Từ 7,0 đến 7,9	B	3,0
	Từ 6,5 đến 6,9	C+	2,5
	Từ 5,5 đến 6,4	C	2,0
Không đạt	Từ 5,0 đến 5,4	D+	1,5
	Từ 4,0 đến 4,9	D	1,0
	Dưới 4,0	F	0,0

7. NỘI DUNG CHƯƠNG TRÌNH ĐÀO TẠO

7.1 Cấu trúc chương trình đào tạo

TT	Khối kiến thức	Số tín chỉ	
		Định hướng ứng dụng	*Định hướng nghiên cứu*
I	**Khối kiến thức chung**	**7**	**7**
II	**Khối kiến thức cơ sở ngành**	**18**	**18**
III	**Khối kiến thức chuyên ngành**	**18**	**20**
IV	**Khối kiến thức tốt nghiệp**	**17**	**15**
	TỔNG CỘNG	**60**	**60**

7.2 Nội dung chương trình

7.2.1. Kiến thức chung

TT	Tên Học phần	Mã số học phần	Số tín chỉ	Loại học phần		Học kỳ	Mã số học phần tiên quyết
				Bắt buộc	*Tự chọn*		
1	Triết học (Philosophy)	BAS4186	3	x		1	
2	Phương pháp nghiên cứu khoa học (Methodologies of scientific research)	SKD4112	2	x		3	
3	Công cụ toán cho công nghệ thông tin (Mathematic Tools for Information Technology)	INT41218	2	x		1	

TT	Tên Học phần	Mã số học phần	Số tín chỉ	Loại học phần		Học kỳ	Mã số học phần tiên quyết
				Bắt buộc	Tự chọn		
	Tổng:		**7**				

7.2.2. Kiến thức cơ sở ngành

7.2.2.1. Định hướng ứng dụng

TT	Tên Học phần	Mã số học phần	Số tín chỉ	Loại học phần		Học kỳ	Mã số học phần tiên quyết
				Bắt buộc	Tự chọn		
4	Mật mã ứng dụng (Applied cryptography)	SEC4341	3	x		1	
5	An toàn hệ thống thông tin (Information systems security)	SEC4342	3	x		1	
6	Quản lý, pháp luật và chính sách ATTT (Information security management, laws and policies)	SEC4343	3	x		2	
	Các học phần tự chọn (chọn 3/7, tổng số 9TC)						
7	Công nghệ Blockchain (Blockchain technology)	SEC4344	3		x	1, 2	SEC4341
8	An toàn điện toán đám mây (Cloud computing security)	SEC4345	3		x	1, 2	SEC4342
9	An toàn IoT (IoT security)	SEC4346	3		x	1, 2	
10	Hạ tầng khoá công khai (Public key infrastructure)	SEC4347	3		x	1, 2	SEC4341
11	Học máy và ứng dụng trong ATTT (Machine learning and applications in information security)	SEC4348	3		x	1, 2	
12	DevOps và DevSecOps (DevOps and DevSecOps)	SEC4349	3		x	1, 2	
13	Các giao thức an toàn và bảo mật (Security protocols)	SEC4350	3		x	1, 2	SEC4341
	Tổng:		**18**				

7.2.2.2. Định hướng nghiên cứu

TT	Tên Học phần	Mã số học phần	Số tín chỉ	Loại học phần		Học kỳ	Mã số học phần tiên quyết
				Bắt buộc	Tự chọn		
4	Mật mã ứng dụng (Applied cryptography)	SEC4341	3	x		1	
5	An toàn hệ thống thông tin (Information systems security)	SEC4342	3	x		1	

TT	Tên Học phần	Mã số học phần	Số tín chỉ	Loại học phần		Học kỳ	Mã số học phần tiên quyết
				Bắt buộc	*Tự chọn*		
6	Quản lý, pháp luật và chính sách ATTT (Information security management, laws and policies)	SEC4343	3	x		2	
	Các học phần tự chọn (chọn 1/3, tổng số 3TC)						
7	Công nghệ Blockchain (Blockchain technology)	SEC4344	3		x	1	SEC4341
8	An toàn điện toán đám mây (Cloud computing security)	SEC4345	3		x	1	SEC4342
9	Học máy và ứng dụng trong ATTT (Machine learning and applications in information security)	SEC4348	3		x	1	
	Các chuyên đề nghiên cứu						
10	Chuyên đề thạc sĩ 1	SEC4351	3	x		2	
11	Chuyên đề thạc sĩ 2	SEC4352	3	x		2	
	Tổng:		**18**				

7.2.3. Kiến thức chuyên ngành

7.2.3.1. Định hướng ứng dụng

TT	Tên Học phần	Mã số học phần	Số tín chỉ	Loại học phần		Học kỳ	Mã số học phần tiên quyết
				Bắt buộc	*Tự chọn*		
14	Phân tích mã độc nâng cao (Advanced malware analysis)	SEC4453	3	x		2	SEC4342
15	Kiểm thử xâm nhập nâng cao (Advanced penetration testing)	SEC4454	3	x		3	SEC4342
16	Giám sát an toàn mạng nâng cao (Advanced network monitoring)	SEC4455	3	x		2	SEC4342
	Các học phần tự chọn (chọn 1/4 học phần 3TC, 3/7 học phần 2TC, tổng số 9TC)						
17	Các chủ đề hiện đại trong ATTT (Modern topics in information security)	SEC4456	3		x	3	
18	Tấn công và phòng thủ mạng (Network attack and defense)	SEC4457	3		x	3	SEC4342
19	Ứng phó và xử lý sự cố bảo mật (Security incident response and handling)	SEC4458	3		x	3	SEC4342
20	Điều tra số (Digital forensics)	SEC4459	3		x	3	SEC4342
21	An toàn web nâng cao (Advanced web security)	SEC4460	2		x	3	

TT	Tên Học phần	Mã số học phần	Số tín chỉ	Loại học phần		Học kỳ	Mã số học phần tiên quyết
				Bắt buộc	Tự chọn		
22	An toàn cơ sở dữ liệu nâng cao (Advanced database security)	SEC4461	2		x	3	
23	Đảm bảo an toàn cho AI (AI security)	SEC4462	2		x	3	SEC4348
24	Mật mã hậu lượng tử (Post-quantum cryptography)	SEC4463	2		x	3	SEC4341
25	Quản trị mạng (Network Administration)	INT44219	2		x	3	
26	Dữ liệu lớn (Big data)	INT44220	2		x	3	
27	Hệ điều hành mạng (Network operating systems)	INT44221	2		x	3	
	Tổng		**18**				

7.2.2.1. Định hướng nghiên cứu

TT	Tên Học phần	Mã số học phần	Số tín chỉ	Loại học phần		Học kỳ	Mã số học phần tiên quyết
				Bắt buộc	Tự chọn		
12	Phân tích mã độc nâng cao (Advanced malware analysis)	SEC4453	3	x		2	SEC4342
13	Kiểm thử xâm nhập nâng cao (Advanced penetration testing)	SEC4454	3	x		3	SEC4342
14	Giám sát an toàn mạng nâng cao (Advanced network monitoring)	SEC4455	3	x		2	SEC4342
	Các học phần tự chọn (chọn 1/4 học phần 3TC, 1/4 học phần 2TC, tổng số 5TC)						
15	Các chủ đề hiện đại trong ATTT (Modern topics in information security)	SEC4456	3		x	3	
16	Tấn công và phòng thủ mạng (Network attack and defense)	SEC4457	3		x	3	SEC4342
17	Ứng phó và xử lý sự cố bảo mật (Security incident response and handling)	SEC4458	3		x	3	SEC4342
18	Điều tra số (Digital forensics)	SEC4459	3		x	3	SEC4342
19	An toàn web nâng cao (Advanced web security)	SEC4460	2		x	3	
20	An toàn cơ sở dữ liệu nâng cao (Advanced database security)	SEC4461	2		x	3	
21	Đảm bảo an toàn cho AI (AI security)	SEC4462	2		x	3	SEC4348

TT	Tên Học phần	Mã số học phần	Số tín chỉ	Loại học phần		Học kỳ	Mã số học phần tiên quyết
				Bắt buộc	Tự chọn		
22	Mật mã hậu lượng tử (Post-quantum cryptography)	SEC4463	2		x	3	SEC4341
	Các chuyên đề nghiên cứu						
23	Chuyên đề thạc sĩ 3	SEC4464	3	x		3	
24	Chuyên đề thạc sĩ 4	SEC4465	3	x		3	
	Tổng		**20**				

7.2.3. Khối kiến thức tốt nghiệp

7.2.3.1. Định hướng ứng dụng

TT	Tên Học phần	Mã số học phần	Số tín chỉ	Loại học phần		Học kỳ	Mã số học phần tiên quyết
				Bắc buộc	Tự chọn		
28	Thực tập tốt nghiệp	SEC4566	8	x		4	
29	Đề án tốt nghiệp	SEC4567	9	x		4	SKD4112
	Tổng		**17**				

7.2.3.2. Định hướng nghiên cứu

TT	Tên Học phần	Mã số học phần	Số tín chỉ	Loại học phần		Học kỳ	Mã số học phần tiên quyết
				Bắc buộc	Tự chọn		
25	Luận văn tốt nghiệp	SEC4568	15	x		4	SKD4112
	Tổng		**15**				

8. KẾ HOẠCH HỌC TẬP CHUẨN

8.1 Kế hoạch học tập chuẩn *(Chi tiết kèm theo)*

8.2 Tiến trình học tập chuẩn *(Chi tiết kèm theo)*

9. MÔ TẢ TÓM TẮT CÁC HỌC PHẦN

9.1. Khối kiến thức chung

TRIẾT HỌC

- Mã học phần: BAS4186
- Số tín chỉ: 3
- Học phần tiên quyết:

- Phân bổ thời lượng: LT[1]: 30 tiết, Bài tập/Thảo luận: 15 tiết, Tự học: 135 giờ

- Tóm tắt nội dung:

Học phần được cấu trúc thành 4 chương: Chương 1 gồm các nội dung về đặc trưng của triết học phương Tây, triết học phương Đông (trong đó có tư tưởng triết học Việt Nam, ở mức giản lược nhất) và triết học Mác; Chương 2 gồm các nội dung nâng cao về triết học Mác-Lênin trong giai đoạn hiện nay và vai trò thế giới quan, phương pháp luận của nó; Chương 3 đi sâu hơn vào quan hệ tương hỗ giữa triết học với các khoa học, làm rõ vai trò thế giới quan và phương pháp luận của triết học đối với sự phát triển khoa học và đối với việc nhận thức, giảng dạy và nghiên cứu các đối tượng thuộc lĩnh vực khoa học tự nhiên và công nghệ; Chương 4 phân tích những vấn đề về vai trò của các khoa học đối với đời sống xã hội.

PHƯƠNG PHÁP NGHIÊN CỨU KHOA HỌC

- Mã học phần: SKD4112

- Số tín chỉ: 2

- Học phần tiên quyết:

- Phân bổ thời lượng: LT: 24 tiết, Bài tập/Thảo luận: 6 tiết, Tự học: 45 giờ

- Tóm tắt nội dung:

Học phần cung cấp cho học viên những kiến thức về các phương pháp tiến hành thực hiện các loại hình nghiên cứu như đề tài khoa học công nghệ các cấp, luận văn tốt nghiệp… một cách có hệ thống và mang tính khoa học. Học phần được cấu trúc thành 6 chương: Tổng quan về khoa học và nghiên cứu khoa học; Trình tự logic của nghiên cứu khoa học; Xây dựng đề cương nghiên cứu khoa học; Phương pháp thu thập, xử lý thông tin; Viết báo cáo và trình bày kết quả nghiên cứu khoa học; Đánh giá công trình nghiên cứu khoa học.

CÔNG CỤ TOÁN CHO CÔNG NGHỆ THÔNG TIN

- Mã học phần: INT41218

- Số tín chỉ: 2

- Học phần tiên quyết:

- Phân bổ thời lượng: LT: 24 tiết, Bài tập/Thảo luận: 6 tiết, Tự học: 45 giờ

- Tóm tắt nội dung:

Học phần cung cấp cho học viên những kiến thức cơ bản liên quan đến các phương pháp toán sử dụng trong công nghệ thông tin, bao gồm Máy Turing và phân lớp các bài toán; Tập mờ, tập thô và ứng dụng; Quá trình Markov và mô hình Markov ẩn; và Các phương pháp toán tối ưu.

[1] LT: Lý thuyết

9.2. Khối kiến thức cơ sở ngành

MẬT MÃ ỨNG DỤNG

- Mã học phần: SEC4341

- Số tín chỉ: 3

- Học phần tiên quyết:

- Phân bổ thời lượng: LT: 25 tiết, Bài tập/Thảo luận/Thực hành: 20 tiết, Tự học: 90 giờ

- Tóm tắt nội dung:

Học phần cung cấp các kiến thức cơ bản và chuyên sâu về mật mã và ứng dụng của mật mã, bao gồm: vai trò, tầm quan trọng của mật mã; các giải thuật mã hóa đối xứng và bất đối xứng thông dụng; các hàm băm phổ biến; các kỹ thuật quản lý và phân phối khóa mật mã; chữ ký số và ứng dụng của chữ ký số; các ứng dụng của mật mã trong bảo mật hệ thống thông tin.

AN TOÀN HỆ THỐNG THÔNG TIN

- Mã học phần: SEC4342

- Số tín chỉ: 3

- Học phần tiên quyết:

- Phân bổ thời lượng: LT: 25 tiết, Bài tập/Thảo luận/Thực hành: 20 tiết, Tự học: 90 giờ

- Tóm tắt nội dung:

Học phần cung cấp các kiến thức cơ bản và chuyên sâu về đảm bảo an toàn cho hệ thống thông tin, bao gồm các nội dung: Tổng quan về đảm bảo an toàn cho hệ thống thông tin; Các điểm yếu, lỗ hổng tồn tại trong hệ thống, gồm cả hệ thống phần cứng và phần mềm; Các mối đe doạ từ đơn giản đến phức tạp đối với hệ thống thông tin, bao gồm các dạng tấn công, xâm nhập và mã độc; Các kỹ thuật, công cụ và giải pháp đảm bảo an toàn cho hệ thống thông tin.

QUẢN LÝ, PHÁP LUẬT VÀ CHÍNH SÁCH ATTT

- Mã học phần: SEC4343

- Số tín chỉ: 2

- Học phần tiên quyết:

- Phân bổ thời lượng: LT: 25 tiết, Bài tập/Thảo luận/Thực hành: 20 tiết, Tự học: 90 giờ

- Tóm tắt nội dung:

Học phần cung cấp cả nền tảng lý thuyết và hiểu biết thực tế về phát triển, triển khai và quản lý các biện pháp bảo mật thông tin để đáp ứng các yêu cầu của tổ chức và cơ quan quản lý. Chương trình giảng dạy bao gồm các tiêu chuẩn bảo mật quốc gia và quốc tế được công nhận rộng rãi, cùng với các quy định về chính sách và pháp lý có liên quan để đảm bảo tuân thủ và áp dụng hiệu quả các giải pháp bảo mật. Ngoài ra, học phần trang bị cho

học viên kiến thức về đánh giá và thử nghiệm bảo mật, bao gồm các phương pháp thử nghiệm bảo mật, đánh giá rủi ro, phân tích kết quả thử nghiệm và kiểm toán bảo mật. Hơn nữa, học viên sẽ khám phá các nguyên tắc và biện pháp để đảm bảo hoạt động hệ thống an toàn, duy trì tính liên tục trong hoạt động doanh nghiệp và ứng phó hiệu quả với các sự cố bảo mật thông tin.

CÔNG NGHỆ BLOCKCHAIN

- Mã học phần: SEC4344

- Số tín chỉ: 3

- Học phần tiên quyết: SEC4341

- Phân bổ thời lượng: LT: 25 tiết, Bài tập/Thảo luận/Thực hành: 20 tiết, Tự học: 90 giờ

- Tóm tắt nội dung:

Học phần cung cấp cho học viên những kiến thức cơ bản và chuyên sâu về Blockchain, bao gồm: vai trò và tầm quan trọng của Blockchain; nền tảng toán học ứng dụng trong Blockchain; các kiến trúc, nguyên lý hoạt động và giao thức của Blockchain; các vấn đề về bảo mật thông tin cho Blockchain, bao gồm ZKP (zero-knowledge-proof), quyền riêng tư, ẩn danh; và một số ứng dụng thực tế của Blockchain.

AN TOÀN ĐIỆN TOÁN ĐÁM MÂY

- Mã học phần: SEC4345

- Số tín chỉ: 3

- Phân bổ thời lượng: LT: 25 tiết, Bài tập/Thảo luận/Thực hành: 20 tiết, Tự học: 90 giờ

- Học phần tiên quyết: SEC4342

- Tóm tắt nội dung:

Học phần cung cấp cho học viên kiến thức cơ bản về đảm bảo an toàn cho điện toán đám mây, bao gồm: khái quát về điện toán đám mây và bảo mật đám mây; các mối đe dọa bảo mật đối với đám mây; bảo mật các tài nguyên tính toán, lưu trữ và mạng cho đám mây; vấn đề quản lý danh tính, truy cập, kiểm toán và mã hóa trên đám mây; vấn đề tuân thủ và quy định đối với đám mây.

AN TOÀN IOT

- Mã học phần: SEC4346

- Số tín chỉ: 3

- Học phần tiên quyết:

- Phân bổ thời lượng: LT: 25 tiết, Bài tập/Thảo luận/Thực hành: 20 tiết, Tự học: 90 giờ

- Tóm tắt nội dung:

Học phần cung cấp cho học viên kiến thức cơ bản về IoT và đảm bảo an toàn cho IoT, bao gồm: Khái quát về IoT; Các giao thức truyền thông trong IoT; Mô hình hóa nguy cơ trong mạng IoT; Các công nghệ đảm bảo an toàn cho mạng IoT; Xây dựng mạng IoT an toàn.

HẠ TẦNG KHOÁ CÔNG KHAI

- Mã học phần: SEC4347

- Số tín chỉ: 3

- Học phần tiên quyết: SEC4341

- Phân bổ thời lượng: LT: 25 tiết, Bài tập/Thảo luận/Thực hành: 20 tiết, Tự học: 90 giờ

- Tóm tắt nội dung:

Học phần cung cấp cho học viên kiến thức cơ bản và nâng cao về Hạ tầng khoá công khai - PKI (Public Key Infrastructure), bao gồm: Tổng quan về PKI và ứng dụng của PKI trong thực tế; Mã hóa khóa công khai; Chứng chỉ số khoá công khai; Cấu trúc và mô hình PKI; Triển khai và quản trị PKI; và Vấn đề chính sách và tuân thủ.

HỌC MÁY VÀ ỨNG DỤNG TRONG ATTT

- Mã học phần: SEC4348

- Số tín chỉ: 3

- Học phần tiên quyết:

- Phân bổ thời lượng: LT: 25 tiết, Bài tập/Thảo luận/Thực hành: 20 tiết, Tự học: 90 giờ

- Tóm tắt nội dung:

Học phần cung cấp cho học viên kiến thức cơ bản và nâng cao về trí tuệ nhân tạo (AI), học máy (ML), học sâu (DL) và ứng dụng ML & DL trong việc giải quyết các vấn đề về an toàn thông tin. Các chủ đề cụ thể của học phần này bao gồm tổng quan về AI, ML và DL; các mô hình học máy truyền thống, học sâu và học chuyển giao; các kỹ thuật tiền xử lý dữ liệu; các mô hình học máy truyền thống cho an toàn thông tin; các mô hình học sâu và học chuyển giao cho an toàn thông tin.

DEVOPS VÀ DEVSECOPS

- Mã học phần: SEC4349

- Số tín chỉ: 3

- Học phần tiên quyết:

- Phân bổ thời lượng: LT: 25 tiết, Bài tập/Thảo luận/Thực hành: 20 tiết, Tự học: 90 giờ

- Tóm tắt nội dung:

Học phần giới thiệu cho người học các khái niệm và thực hành thiết yếu của DevOps và DevSecOps, chuẩn bị cho người học các vai trò trong tương lai trong ngành công nghệ. Đặc biệt, học phần cung cấp cho người học các công cụ và công nghệ chính được sử dụng trong môi trường DevOps, để có được kinh nghiệm thực tế với các đường ống tích hợp liên

tục và triển khai liên tục (CI/CD); kiến trúc DevOps và DevSecOps; và các thực hành phát triển an toàn.

CÁC GIAO THỨC AN TOÀN VÀ BẢO MẬT

- Mã học phần: SEC4350

- Số tín chỉ: 3

- Học phần tiên quyết: SEC4341

- Phân bổ thời lượng: LT: 25 tiết, Bài tập/Thảo luận/Thực hành: 20 tiết, Tự học: 90 giờ

- Tóm tắt nội dung:

Học phần cung cấp cho học viên kiến thức nâng cao về các giao thức bảo mật thông tin và đảm bảo an toàn cho hệ thống và mạng, bao gồm các giao thức xác thực người dùng; các bộ giao thức bảo mật thông tin truyền, bao gồm Transport Layer Security (TLS) and Secure Sockets Layer (SSL), Internet Protocol Security (IPsec), Secure shell (SSH), Datagram Transport Layer Security (DTLS) và Pretty Good Privacy (PGP).

9.3. Khối kiến thức chuyên ngành

PHÂN TÍCH MÃ ĐỘC NÂNG CAO

- Mã học phần: SEC4453

- Số tín chỉ: 3

- Học phần tiên quyết: SEC4342

- Phân bổ thời lượng: LT: 25 tiết, Bài tập/Thảo luận/Thực hành: 20 tiết, Tự học: 90 giờ

- Tóm tắt nội dung:

Học phần cung cấp cho học viên kiến thức nâng cao về phân tích mã độc, bao gồm: Tổng quan về mã độc và môi trường phân tích an toàn; Phân tích tĩnh nâng cao; Phân tích động nâng cao; Kỹ thuật phân tích mã độc được bảo vệ; Phân tích mạng và hạ tầng C&C; Dịch ngược nâng cao; Phân tích mã độc thực tế & Case Study; Phòng thủ & phát hiện nâng cao.

KIỂM THỬ XÂM NHẬP NÂNG CAO

- Mã học phần: SEC4454

- Số tín chỉ: 3

- Học phần tiên quyết: SEC4342

- Phân bổ thời lượng: LT: 25 tiết, Bài tập/Thảo luận/Thực hành: 20 tiết, Tự học: 90 giờ

- Tóm tắt nội dung:

Học phần cung cấp cho học viên kiến thức nâng cao về kiểm thử xâm nhập, bao gồm: Giới thiệu và qui trình kiểm thử xâm nhập; Recon & OSINT nâng cao; Quét & fingerprinting mạng nâng cao; Khai thác hạ tầng & chaining exploit; Tấn công Active Directory (AD) nâng cao; Post-exploitation Windows & kỹ thuật ẩn mình; Linux / Cloud hậu khai thác;

Kiểm thử ứng dụng web và API nâng cao; Mô phỏng Red Team và tấn công đối nghịch; Phát hiện và tăng cường an toàn.

GIÁM SÁT AN TOÀN MẠNG NÂNG CAO

- Mã học phần: SEC4455

- Số tín chỉ: 3

- Học phần tiên quyết: SEC4342

- Phân bổ thời lượng: LT: 25 tiết, Bài tập/Thảo luận/Thực hành: 20 tiết, Tự học: 90 giờ

- Tóm tắt nội dung:

Học phần cung cấp cho học viên kiến thức nâng cao về giám sát an toàn mạng, bao gồm các thành phần hệ thống giám sát, thu thập dữ liệu và các kỹ thuật phát hiện xâm nhập. Học phần cũng bao gồm các kỹ thuật phát hiện dựa trên chữ ký và dựa trên bất thường, các công cụ bảo mật để phân tích mối đe dọa và tích hợp với cơ sở hạ tầng bảo mật. Thông qua các bài tập thực hành và các dự án nhóm, học viên sẽ có được các kỹ năng thực tế trong việc triển khai và quản lý các hệ thống giám sát mạng.

CÁC CHỦ ĐỀ HIỆN ĐẠI TRONG ATTT

- Mã học phần: SEC4456

- Số tín chỉ: 3

- Học phần tiên quyết:

- Phân bổ thời lượng: LT: 25 tiết, Bài tập/Thảo luận/Thực hành: 20 tiết, Tự học: 90 giờ

- Tóm tắt nội dung:

Học phần cung cấp cho học viên kiến thức về các các chủ đề cập nhật và hiện đại trong an toàn thông tin, như hệ thống tường lửa thế hệ mới, IDS/IPS thế hệ mới có tích hợp AI, các giao thức và hệ thống xác thực tiên tiến, các dạng tấn công vào các mô hình AI và phòng chống, các phương pháp tấn công và phòng thủ mạng tiên tiến, các dạng mã độc, botnet mới và phương pháp phòng chống, phát hiện.

TẤN CÔNG VÀ PHÒNG THỦ MẠNG

- Mã học phần: SEC4457

- Số tín chỉ: 2

- Học phần tiên quyết: SEC4302

- Phân bổ thời lượng: LT: 25 tiết, Bài tập/Thảo luận/Thực hành: 20 tiết, Tự học: 90 giờ

- Tóm tắt nội dung:

Học phần cung cấp các kiến thức chuyên sâu về các tấn công và phòng thủ mạng, bao gồm các nội dung: Các nguy cơ và lỗ hổng trong bảo mật trong các giao thức và thiết bị mạng; Các kỹ thuật do thám, rà quét và xâm nhập mạng; và Các giải pháp phòng ngừa và ngăn chặn tấn công mạng.

ỨNG PHÓ VÀ XỬ LÝ SỰ CỐ BẢO MẬT

- Mã học phần: SEC4458

- Số tín chỉ: 2

- Học phần tiên quyết: SEC4342

- Phân bổ thời lượng: LT: 25 tiết, Bài tập/Thảo luận/Thực hành: 20 tiết, Tự học: 90 giờ

- Tóm tắt nội dung:

Học phần cung cấp cho học viên những kiến thức cơ bản và nâng cao về ứng phó và xử lý sự cố bảo mật, bao gồm: Khái quát về sự cố bảo mật và ứng phó, xử lý sự cố; Các chiến lược ứng phó, khôi phục sau sự cố và đảm bảo hoạt động liên tục; Lập kế hoạch ứng phó, xử lý sự cố; Phát hiện và ứng phó sự cố; Khôi phục, bảo trì và điều tra sự cố.

ĐIỀU TRA SỐ

- Mã học phần: SEC4459

- Số tín chỉ: 3

- Học phần tiên quyết: SEC4342

- Phân bổ thời lượng: LT: 25 tiết, Bài tập/Thảo luận/Thực hành: 20 tiết, Tự học: 90 giờ

- Tóm tắt nội dung:

Học phần cung cấp kiến thức cơ bản về pháp y kỹ thuật số, tập trung vào các thủ tục điều tra pháp y, thu thập dữ liệu, phân tích pháp y, xác thực và viết báo cáo. Học phần khám phá các kỹ thuật thu thập, phân tích và diễn giải bằng chứng kỹ thuật số từ nhiều nguồn khác nhau, bao gồm hệ điều hành, thiết bị di động, mạng và dịch vụ trực tuyến. Học phần cũng bao gồm các công cụ pháp y, kỹ thuật phục hồi dữ liệu, giải quyết các phương pháp ẩn dữ liệu và các biện pháp thực hành tốt nhất để ghi lại các phát hiện trong báo cáo cho các thủ tục tố tụng pháp lý.

AN TOÀN WEB NÂNG CAO

- Mã học phần: SEC4460

- Số tín chỉ: 2

- Học phần tiên quyết:

- Phân bổ thời lượng: LT: 15 tiết, Bài tập/Thảo luận/Thực hành: 15 tiết, Tự học: 45 giờ

- Tóm tắt nội dung:

Học phần cung cấp các kiến thức chuyên sâu về bảo mật cho các website, ứng dụng web, bao gồm: Các yêu cầu bảo mật các ứng dụng web; Các nguy cơ, điểm yếu và lỗ hổng bảo mật trong các ứng dụng Web; Các phương pháp tiếp cận bảo mật các ứng dụng Web; Các dạng tấn công lên các ứng dụng Web; Các biện pháp bảo mật máy chủ, ứng dụng web và trình duyệt web; Vấn đề bảo mật trong phát triển và triển khai ứng dụng web

AN TOÀN CƠ SỞ DỮ LIỆU NÂNG CAO

- Mã học phần: SEC4461

- Số tín chỉ: 2

- Học phần tiên quyết:

- Phân bổ thời lượng: LT: 15 tiết, Bài tập/Thảo luận/Thực hành: 15 tiết, Tự học: 45 giờ

- Tóm tắt nội dung:

Học phần cung cấp các kiến thức chuyên sâu về bảo mật cho cơ sở dữ liệu bao (CSDL) gồm: Các yêu cầu bảo mật CSDL, mô hình tổng quát bảo mật CSDL, các dạng tấn công thường gặp vào CSDL; Các cơ chế bảo mật CSDL; Vấn đề sao lưu, khôi phục dự phòng; Vấn đề kiểm toán và giám sát hoạt động của CSDL.

ĐẢM BẢO AN TOÀN CHO AI

- Mã học phần: SEC4462

- Số tín chỉ: 2

- Học phần tiên quyết: SEC4348

- Phân bổ thời lượng: LT: 15 tiết, Bài tập/Thảo luận/Thực hành: 15 tiết, Tự học: 45 giờ

- Tóm tắt nội dung:

Học phần cung cấp cho học viên kiến thức cơ bản và nâng cao về các cuộc tấn công mô hình AI và các chiến lược phòng thủ của chúng, bao gồm các rủi ro, lỗ hổng và thách thức về quyền riêng tư trong các mô hình AI, các kỹ thuật tấn công đối nghịch và các giải pháp phòng ngừa và ứng phó.

MẬT MÃ HẬU LƯỢNG TỬ

- Mã học phần: SEC4463

- Số tín chỉ: 2

- Học phần tiên quyết: SEC4341

- Phân bổ thời lượng: LT: 15 tiết, Bài tập/Thảo luận/Thực hành: 15 tiết, Tự học: 45 giờ

- Tóm tắt nội dung:

Học phần cung cấp các kiến thức cơ bản và nâng cao về mật mã hậu lượng tử, bao gồm: Tổng quan về mật mã hậu lượng tử; Cơ sở toán học của mật mã hậu lượng tử; Các lược đồ dựa trên lưới (Lattice-based schemes); Các lược đồ dựa trên mã, băm và đa biến (Code-based, hash-based và multivariate schemes); Các thuật toán khác & lịch sử thay đổi mật mã hậu lượng tử; Các giao thức và tích hợp mật mã hậu lượng tử; Thực thi, triển khai và đánh giá; Quản lý khoá và vòng đời; Các vector tấn công và thám mã.

QUẢN TRỊ MẠNG

- Mã học phần: INT44219

- Số tín chỉ: 2

- Học phần tiên quyết:

- Phân bổ thời lượng: LT: 24 tiết, Bài tập/Thảo luận/Thực hành: 6 tiết, Tự học: 45 giờ

- Tóm tắt nội dung:

Học phần cung cấp cho học viên kiến thức cơ bản và chuyên sâu về quản trị hệ thống mạng, bao gồm Tổng quan về quản trị mạng; Kiến trúc mạng và thiết bị mạng; Địa chỉ mạng và dịch vụ mạng cơ bản; Hệ điều hành mạng và dịch vụ máy chủ; Quản trị và cấu hình mạng; Giám sát, vận hành và tối ưu mạng; An toàn và bảo mật mạng; và Tự động hóa và quản trị mạng hiện đại.

DỮ LIỆU LỚN

- Mã học phần: INT44220

- Số tín chỉ: 2

- Học phần tiên quyết:

- Phân bổ thời lượng: LT: 24 tiết, Bài tập/Thảo luận/Thực hành: 6 tiết, Tự học: 45 giờ

- Tóm tắt nội dung:

Học phần cung cấp cho học viên kiến thức cơ bản và chuyên sâu về dữ liệu lớn, bao gồm Tổng quan về dữ liệu lớn; Kiến trúc hệ thống dữ liệu lớn; Thu thập và tiền xử lý dữ liệu lớn; Lưu trữ dữ liệu lớn; Xử lý và phân tích dữ liệu lớn; Xử lý dữ liệu thời gian thực; Truy vấn, trực quan và khai thác dữ liệu; An toàn và bảo mật dữ liệu lớn; Xu hướng và triển vọng dữ liệu lớn.

HỆ ĐIỀU HÀNH MẠNG

- Mã học phần: INT44221

- Số tín chỉ: 2

- Học phần tiên quyết:

- Phân bổ thời lượng: LT: 24 tiết, Bài tập/Thảo luận/Thực hành: 6 tiết, Tự học: 45 giờ

- Tóm tắt nội dung:

Học phần cung cấp cho người học các kiến thức cơ bản và chuyên sâu về hệ điều hành mạng và các dịch vụ của nó, bao gồm: Giới thiệu về Hệ điều hành mạng; Hệ thống file phân tán; Các cơ chế giao tiếp và điều độ các tiến trình phân tán; Thời gian và đồng bộ hoá thời gian trong hệ thống phân tán; Giới thiệu về công nghệ ảo hóa; Tổng quan về Điện toán đám mây.

CHUYÊN ĐỀ THẠC SĨ 1, 2, 3, 4

- Mã học phần: SEC4351, SEC4352, SEC4464, SEC4465

- Số tín chỉ: 3

- Học phần tiên quyết:

- Phân bổ thời lượng: LT: 5 tiết, Bài tập/Thảo luận/Thực hành: 40 tiết, Tự học: 90 giờ

- Tóm tắt nội dung:

Các học phần chuyên đề an toàn thông tin cung cấp cho học viên kiến thức và kỹ năng chuyên sâu về:

- Đảm bảo an toàn cho các phần mềm, bao gồm đảm bảo an toàn cho hệ điều hành, an toàn cho các dịch vụ và ứng dụng; Vấn đề rà quét phát hiện và khắc phục các lỗ hổng bảo mật phần mềm;
- Đảm bảo an ninh mạng, bao gồm các điểm yếu và lỗ hổng trong bảo mật các giao thức và hệ thống mạng, các kỹ thuật tấn công mạng, các giải pháp phòng ngừa và đáp trả tấn công.

Các học phần trên được thực hiện theo hình thức dự án (project) nhóm để thực hiện các nhiệm vụ cụ thể có liên quan đến đảm bảo an toàn cho các phần mềm cũng như đảm bảo an ninh mạng.

9.4. Khối kiến thức tốt nghiệp

THỰC TẬP TỐT NGHIỆP

- Mã học phần: SEC4566

- Số tín chỉ: 8

- Học phần tiên quyết:

- Tóm tắt nội dung:

Học phần hỗ trợ học viên áp dụng các kiến thức chuyên ngành đã học vào giải quyết các vấn đề thực tế có liên quan đến ATTT tại các doanh nghiệp, nhằm rèn luyện kỹ năng phân tích, giải quyết vấn đề và nâng cao trải nghiệm thực tế của học viên.

ĐỀ ÁN TỐT NGHIỆP

- Mã học phần: SEC4567

- Số tín chỉ: 9

- Học phần tiên quyết: SKD4112

- Tóm tắt nội dung:

Thực hiện học phần này, học viên áp dụng các kiến thức, kỹ năng chuyên ngành đã học và khả năng nghiên cứu để giải quyết trọn vẹn một vấn đề lý thuyết hoặc kết hợp thực hành có liên quan đến lĩnh vực ATTT nhằm nâng cao kỹ năng tư duy, phân tích và giải quyết vấn đề, gồm cả kỹ năng viết báo cáo và trình bày, demo kết quả nghiên cứu.

LUẬN VĂN TỐT NGHIỆP

- Mã học phần: SEC4568

- Số tín chỉ: 15

- Học phần tiên quyết: SKD4112

- Tóm tắt nội dung:

Thực hiện học phần này, học viên áp dụng các kiến thức, kỹ năng chuyên ngành đã học và khả năng nghiên cứu để giải quyết trọn vẹn một vấn đề lý thuyết hoặc kết hợp thực hành có liên quan đến lĩnh vực ATTT nhằm nâng cao kỹ năng tư duy, phân tích và giải quyết vấn đề, gồm cả kỹ năng viết báo cáo và trình bày, demo kết quả nghiên cứu. Kết quả của luận văn phải được công bố trên các tạp chí hoặc hội thảo chuyên ngành có phản biện, có điểm công trình khoa học đạt 0.5 điểm theo quy định của Hội đồng chức danh giáo sư nhà nước.

10. MA TRẬN LIÊN KẾT GIỮA CÁC HỌC PHẦN VỚI CHUẨN ĐẦU RA *(Chi tiết kèm theo)*.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

PGS.TS Trần Quang Anh

PHỤ LỤC 1

DANH MỤC NGÀNH ĐÚNG, PHÙ HỢP, NGÀNH GẦN VÀ CÁC MÔN HỌC BỔ SUNG KIẾN THỨC TUYỂN SINH TRÌNH ĐỘ THẠC SĨ NGÀNH AN TOÀN THÔNG TIN

TT	Chuyên ngành tuyển sinh	Ngành đúng, phù hợp	Ngành gần và các môn học bổ sung kiến thức			Ghi chú
			Ngành gần	Môn bổ sung kiến thức	Số tiết	
1	**An toàn thông tin** Mã số chuyên ngành: 8480202	- An toàn thông tin - An ninh mạng - Hoặc các ngành/chuyên ngành không có tên nêu trên nhưng có chương trình đào tạo khác với chương trình đào tạo đại học ngành An toàn thông tin của Học viện dưới 10% tổng số tiết hoặc đơn vị học trình hoặc tín chỉ của khối kiến thức ngành.	**Nhóm 1: Các ngành, chuyên ngành gần** - Công nghệ thông tin - Hệ thống thông tin - Kỹ thuật phần mềm - Công nghệ phần mềm - Truyền thông và mạng máy tính - Truyền dữ liệu và mạng máy tính - Khoa học máy tính - Khoa học dữ liệu - Trí tuệ nhân tạo - Kỹ thuật mật mã - Hoặc các ngành/chuyên ngành không có tên trong Nhóm 1 nêu trên nhưng có chương trình đào tạo khác với chương trình đào tạo đại học ngành An toàn thông tin của Học viện từ 10-20% tổng số tiết hoặc đơn vị học trình hoặc tín chỉ của khối kiến thức ngành	**Nhóm 1:**		
				1. Cơ sở an toàn thông tin	45	
				2. Mật mã học cơ sở	45	
				3. Hệ điều hành Windows và Linux/Unix	45	
				4. Mạng máy tính	45	
				Thí sinh có thể được miễn một số môn bổ sung kiến thức nếu chương trình đào tạo đã có môn học với nội dung tương đương các môn học trên trong chương trình đào tạo đại học ngành An toàn thông tin của Học viện.		
			Nhóm 2: Các ngành, chuyên ngành khác - Kỹ thuật điện tử, truyền thông; - Kỹ thuật điện tử viễn thông; - Công nghệ kỹ thuật điện tử, truyền thông; - Công nghệ kỹ thuật điện tử viễn thông; - Kỹ thuật máy tính; - Công nghệ kỹ thuật máy tính;	**Nhóm 2:**		
				Ngoài 4 môn học như Nhóm 1 phải học thêm 3 môn sau:		
				1. Cấu trúc dữ liệu và giải thuật	45	
				2. Python cho An toàn thông tin	45	
				3. Hợp ngữ và dịch ngược	45	

TT	Chuyên ngành tuyển sinh	Ngành đúng, phù hợp	Ngành gần và các môn học bổ sung kiến thức			Ghi chú
			Ngành gần	Môn bổ sung kiến thức	Số tiết	
			- Điện tử tin học; - Kỹ thuật điều khiển và tự động hóa; - Công nghệ kỹ thuật điều khiển và tự động hóa - Kỹ thuật điện, điện tử; - Công nghệ kỹ thuật điện, điện tử; - Kỹ thuật điện tử - Tin học quản lý; - Toán tin; - Tin học ứng dụng - Toán - Tin học; - Hệ thống thông tin kinh tế - Hoặc các ngành/chuyên ngành không có tên trong Nhóm 1, 2 nêu trên nhưng có chương trình đào tạo khác với chương trình đào tạo đại học ngành An toàn thông tin của Học viện ***từ 20-40%*** tổng số tiết hoặc đơn vị học trình hoặc tín chỉ của khối kiến thức ngành	Thí sinh có thể được miễn một số môn bổ sung kiến thức nếu chương trình đào tạo đã có môn học với nội dung tương đương các môn học trên trong chương trình đào tạo đại học ngành An toàn thông tin của Học viện.		

PHỤ LỤC 2
DANH MỤC CÁC MÔN HỌC DÙNG XÉT TUYỂN TRÌNH ĐỘ THẠC SĨ NGÀNH AN TOÀN THÔNG TIN

TT	Môn Cơ sở ngành *(Chọn 1 trong 3 môn)*		Môn Chuyên ngành *(Chọn 1 trong 3 môn)*	
	Tên môn học	***Số TC***	***Tên môn học***	***Số TC***
1.	Mạng máy tính	3	An toàn mạng	3
2.	Cơ sở an toàn thông tin	3	Kiểm thử xâm nhập	3
3.	Mật mã học cơ sở	3	An toàn ứng dụng web và cơ sở dữ liệu	3

KẾ HOẠCH & TIẾN TRÌNH HỌC TẬP CHUẨN
THẠC SĨ NGÀNH AN TOÀN THÔNG TIN - ĐỊNH HƯỚNG ỨNG DỤNG

TT	Tên môn học/học phần	Số TC	Học kỳ
1	Triết học	3	HK1
2	Công cụ toán cho công nghệ thông tin	2	HK1
3	Mật mã ứng dụng	3	HK1
4	An toàn hệ thống thông tin	3	HK1
5	Tự chọn cơ sở ngành A1	3	HK1
		14	
6	Quản lý, pháp luật và chính sách ATTT	3	HK2
7	Phân tích mã độc nâng cao	3	HK2
8	Giám sát an toàn mạng nâng cao	3	HK2
9	Tự chọn cơ sở ngành A2	3	HK2
10	Tự chọn cơ sở ngành A3	3	HK2
		15	

TT	Tên môn học/học phần	Số TC	Học kỳ
1	Kiểm thử xâm nhập nâng cao	3	HK3
2	Tự chọn chuyên ngành B1	3	HK3
3	Tự chọn chuyên ngành C1	2	HK3
4	Tự chọn chuyên ngành C2	2	HK3
5	Tự chọn chuyên ngành C3	2	HK3
6	Phương pháp nghiên cứu khoa học	2	HK3
		14	
7	Thực tập tốt nghiệp	8	HK4
8	Đề án tốt nghiệp	9	HK4
		17	
	TỔNG CỘNG:	**60**	

	A Các học phần tự chọn cơ sở ngành	
1	*Công nghệ Blockchain*	3
2	*An toàn điện toán đám mây*	3
3	*An toàn cho IoT*	3
4	*Hạ tầng khoá công khai*	3
5	*Học máy và ứng dụng trong ATTT*	3
6	*DevOps và DevSecOps*	3
7	*Các giao thức an toàn và bảo mật*	3

	B Các học phần tự chọn chuyên ngành	
1	*Các chủ đề hiện đại trong ATTT*	3
2	*Tấn công và phòng thủ mạng*	3
3	*Ứng phó và xử lý sự cố bảo mật*	3
4	*Điều tra số*	3

	C Các học phần tự chọn chuyên ngành	
1	*An toàn web nâng cao*	2
2	*An toàn cơ sở dữ liệu nâng cao*	2
3	*Mật mã hậu lượng tử*	2
4	*Đảm bảo an toàn cho AI*	2
5	*Quản trị mạng*	2
6	*Dữ liệu lớn*	2
7	*Hệ điều hành mạng*	2

KẾ HOẠCH & TIẾN TRÌNH HỌC TẬP CHUẨN
THẠC SĨ NGÀNH AN TOÀN THÔNG TIN - ĐỊNH HƯỚNG NGHIÊN CỨU

TT	Tên môn học/học phần	Số TC	Học kỳ
1	Triết học	3	HK1
2	Công cụ toán cho công nghệ thông tin	2	HK1
3	Mật mã ứng dụng	3	HK1
4	An toàn hệ thống thông tin	3	HK1
5	Tự chọn cơ sở ngành A1	3	HK1
		14	
6	Quản lý, pháp luật và chính sách ATTT	3	HK2
7	Phân tích mã độc nâng cao	3	HK2
8	Giám sát an toàn mạng nâng cao	3	HK2
9	Chuyên đề thạc sĩ 1	3	HK2
10	Chuyên đề thạc sĩ 2	3	HK2
		15	

TT	Tên môn học/học phần	Số TC	Học kỳ
1	Kiểm thử xâm nhập nâng cao	3	HK3
2	Tự chọn chuyên ngành B1	3	HK3
3	Tự chọn chuyên ngành C1	2	HK3
4	Chuyên đề thạc sĩ 3	3	HK3
5	Chuyên đề thạc sĩ 4	3	HK3
6	Phương pháp nghiên cứu khoa học	2	HK3
		16	
6	Luận văn tốt nghiệp	15	HK4
		15	
	TỔNG CỘNG CTĐT:	**60**	

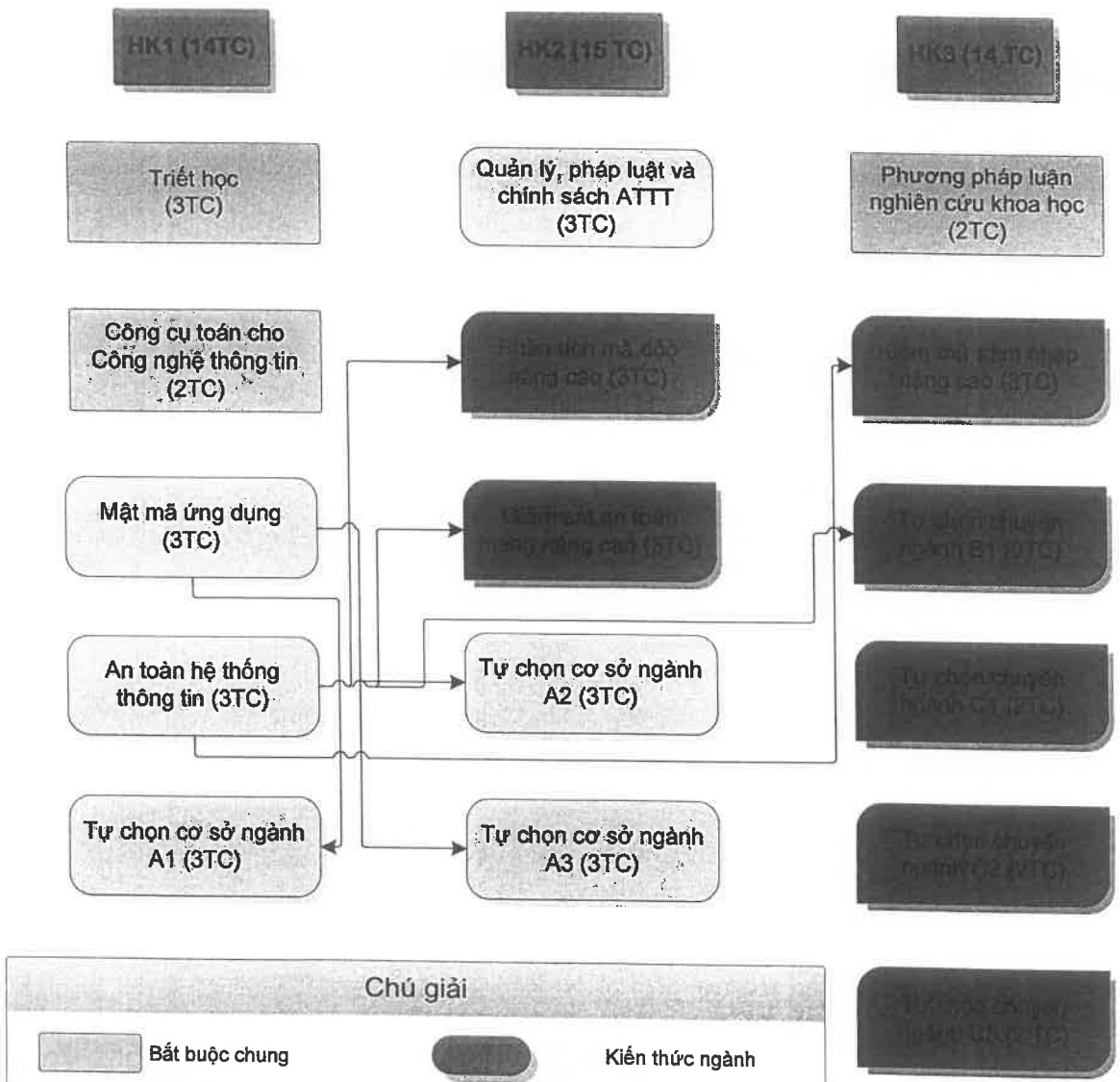
A	***Các học phần tự chọn cơ sở ngành***	
1	*Công nghệ Blockchain*	*3*
2	*An toàn điện toán đám mây*	*3*
3	*Học máy và ứng dụng trong ATTT*	*3*

B	***Các học phần tự chọn chuyên ngành***	
1	*Các chủ đề hiện đại trong ATTT*	*3*
2	*Tấn công và phòng thủ mạng*	*3*
3	*Ứng phó và xử lý sự cố bảo mật*	*3*
4	*Điều tra số*	*3*

C	***Các học phần tự chọn chuyên ngành***	
1	*An toàn web nâng cao*	*2*
2	*An toàn cơ sở dữ liệu nâng cao*	*2*
3	*Mật mã hậu lượng tử*	*2*
4	*Đảm bảo an toàn cho AI*	*2*

TIẾN TRÌNH HỌC TẬP CHUẨN

TRÌNH ĐỘ THẠC SĨ, NGÀNH AN TOÀN THÔNG TIN - Định hướng ứng dụng



A. Các học phần tự chọn cơ sở ngành:

1. Công nghệ Blockchain (3TC);
2. An toàn điện toán đám mây (3TC);
3. An toàn cho IoT (3TC);
4. Hạ tầng khóa công khai (3TC);
5. Học máy và ứng dụng trong ATTT (3TC);
6. DevOps và DevSecOps (3TC);
7. Các giao thức an toàn bảo mật (3TC).

B. Các học phần tự chọn chuyên ngành:

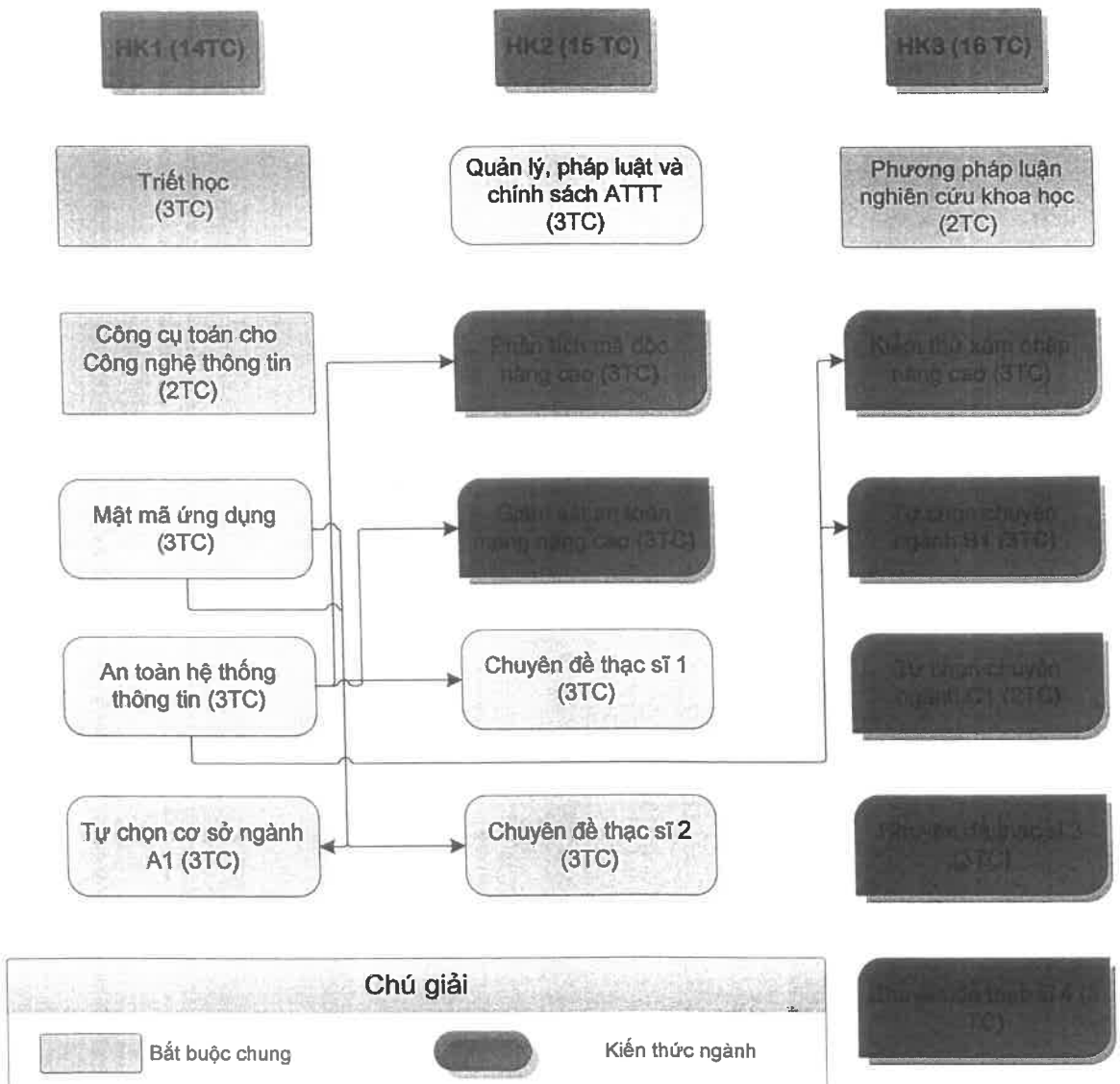
1. Các chủ đề hiện đại trong ATTT (3TC);
2. Tấn công và phòng thủ mạng (3TC);
3. Ứng phó và xử lý sự cố bảo mật (3TC);
4. Điều tra số (3TC).

C. Các học phần tự chọn chuyên ngành:

1. An toàn web nâng cao (2TC);
2. An toàn cơ sở dữ liệu nâng cao (2TC);
3. Mật mã hậu lượng tử (2TC);
4. Đảm bảo an toàn AI (2TC);
5. Quản trị mạng (2TC)
6. Dữ liệu lớn (2TC);
7. Hệ điều hành mạng (2TC).

TIẾN TRÌNH HỌC TẬP CHUẨN

TRÌNH ĐỘ THẠC SĨ, NGÀNH AN TOÀN THÔNG TIN - Định hướng nghiên cứu



A. Các học phần tự chọn cơ sở ngành:

1. Công nghệ Blockchain (3TC);
2. An toàn điện toán đám mây (3TC);
3. Học máy và ứng dụng trong ATTT (3TC);

B. Các học phần tự chọn chuyên ngành:

1. Các chủ đề hiện đại trong ATTT (3TC);
2. Tấn công và phòng thủ mạng (3TC);
3. Ứng phó và xử lý sự cố bảo mật (3TC);
4. Điều tra số (3TC).

C. Các học phần tự chọn chuyên ngành:

1. An toàn web nâng cao (2TC);
2. An toàn cơ sở dữ liệu nâng cao (2TC);
3. Mật mã hậu lượng tử (2TC);
4. Đảm bảo an toàn AI (2TC).

MA TRẬN LIÊN KẾT GIỮA CÁC HỌC PHẦN VỚI CHUẨN ĐẦU RA

TT	TÊN HỌC PHẦN	CHUẨN ĐẦU RA				
		PLO1	PLO2	PLO3	PLO4	PLO5
Kiến thức chung						
1	Triết học			I(Y)		
2	Công cụ toán cho công nghệ thông tin	I(X, A)				
3	Phương pháp nghiên cứu khoa học	I(Y)	I(Y)			
Kiến thức cơ sở ngành						
4	Mật mã ứng dụng	I(X, A)	I(X, A)		I(X, A)	
5	An toàn hệ thống thông tin	R(X, A)	I(X, A)	I(X, A)		
6	Quản lý, pháp luật và chính sách ATTT			R(X, A)	R(X, A)	R(X, A)
7	Chuyên đề thạc sĩ 1	R(X, A)	R(X, A)		I(X, A)	I(X, A)
8	Chuyên đề thạc sĩ 2	E(X, A)	R(X, A)		I(X, A)	I(X, A)
Các học phần tự chọn						
9	Công nghệ Blockchain	R(X, A)	R(X, A)		I(X, A)	I(X, A)
10	An toàn điện toán đám mây	R(X, A)	R(X, A)		I(X, A)	I(X, A)
11	An toàn IoT	R(X, A)	R(X, A)		I(X, A)	I(X, A)
12	Hạ tầng khoá công khai	R(X, A)	R(X, A)	I(X, A)		
13	Học máy và ứng dụng trong ATTT	E(X, A)	R(X, A)		I(X, A)	I(X, A)
14	DevOps và DevSecOps	R(X, A)	R(X, A)		I(X, A)	I(X, A)
15	Các giao thức an toàn và bảo mật	R(X, A)	R(X, A)	I(X, A)		
Kiến thức chuyên ngành						
16	Phân tích mã độc nâng cao		R(X, A)	R(X, A)	R(X, A)	R(X, A)
17	Kiểm thử xâm nhập nâng cao		R(Y, A)	E(X, A)	E(X, A)	R(X, A)
18	Giám sát an toàn mạng nâng cao			R(X, A)	R(X, A)	R(X, A)
19	Chuyên đề thạc sĩ 3	E(X, A)	E(X, A)	R(Y, A)		E(X, A)
20	Chuyên đề thạc sĩ 4		E(X, A)	E(X, A)		E(X, A)
Các học phần tự chọn						
21	Các chủ đề hiện đại trong ATTT		E(X, A)	R(Y, A)		E(X, A)
22	Tấn công và phòng thủ mạng		E(X, A)	R(Y, A)		E(X, A)
23	Ứng phó và xử lý sự cố bảo mật		E(X, A)	R(Y, A)		E(X, A)
24	Điều tra số		E(X, A)	R(Y, A)		E(X, A)
25	An toàn web nâng cao		E(X, A)	R(Y, A)		E(X, A)
26	An toàn cơ sở dữ liệu nâng cao		E(X, A)	R(Y, A)		E(X, A)
27	Đảm bảo an toàn cho AI		E(X, A)	R(Y, A)		E(X, A)
28	Mật mã hậu lượng tử		R(Y, A)		E(X, A)	E(Y, A)
29	Quản trị mạng		R(Y, A)		E(X, A)	E(Y, A)
30	Dữ liệu lớn		R(Y, A)		E(X, A)	E(Y, A)
31	Hệ điều hành mạng		R(Y, A)		E(X, A)	E(Y, A)
32	**Thực tập tốt nghiệp**	E(X, A)	E(X, A)	E(X, A)		R(Y)
33	**Đề án tốt nghiệp thạc sĩ**	E(X, A)	E(X, A)	E(X, A)		E(X, A)
34	**Luận văn tốt nghiệp thạc sĩ**	E(X, A)	E(X, A)	E(X, A)		E(X, A)

Ghi chú:

I,R,E: mức độ đóng góp của học phần, tương ứng: Giới thiệu, cơ bản (I), Củng cố, phát triển thêm (R), Nâng cao, hoàn thiện (E)

X: đóng góp trực tiếp

Y: đóng góp gián tiếp

A: dùng để đo lường đóng góp vào PLO