|  |  |
| --- | --- |
| TRƯỜNG ĐẠI HỌC HẠ LONG | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** |
| **KHOA CÔNG NGHỆ THÔNG TIN** | **Độc lập - Tự do - Hạnh phúc** |

**ĐỀ CƯƠNG CHI TIẾT HỌC PHẦN**

**Trình độ đào tạo: Đại học Ngành: Khoa học máy tính**

**1. Thông tin chung về học phần**

|  |  |
| --- | --- |
| ***1.1. Mã học phần:*** | IT608012 |
| ***1.2. Tên học phần:*** | Nhập môn An toàn thông tin |
| ***1.3. Tên tiếng Anh:*** | Introduction to information security |
| ***1.4. Số tín chỉ:*** | 3 |
| ***1.5. Phân bố thời gian*** |  |
| **-** Lý thuyết: | 45 giờ (3 tín chỉ) |
| - Thực hành: | 0 giờ (0 tín chỉ) |
| - Tự học: | 90 giờ |
| ***1.6. Quản lí, phụ trách học phần*** |  |
| - Khoa quản lí học phần: | Khoa Công nghệ thông tin |
| - Giảng viên phụ trách chính: | Th.S Trịnh Thị Vân |
| - Danh sách giảng viên cùng giảng dạy: |  |
| ***1.7. Điều kiện tham gia học phần*** |  |
| **-** Học phần tiên quyết: | Không |
| - Học phần học trước: | Mạng máy tính |
| - Học phần song hành: | Không |

**2. Mục tiêu học phần**

***2.1. Mục tiêu chung[[1]](#endnote-1)***

Sau khi học xong học phần, sinh viên có kiến thức về những nguyên nhân dẫn đến mất an toàn thông tin trong hệ thống thông tin. Từ đó, giới thiệu về cách lưu trữ hệ thống thông tin trên các thiết bị lưu trữ cũng như cách phòng chống virus và một số biện pháp, phương án an toàn thông tin như hệ thống tường lửa, hệ thống Proxy, IDS/IPS,... Ngoài ra, học phần cũng trang bị một số kiến thức về phương thức mã hóa và giải mã dữ liệu, một số kỹ thuật tấn công hệ thống thông tin, xây dựng và bảo vệ hệ thống thông tin trên máy tính, chính sách và pháp luật an toàn thông tin,...

***2.2. Mục tiêu cụ thể (COs)***

*2.2.1. Về kiến thức*

- CO 1: Có kiến thức về nguyên nhân dẫn đến mất an toàn trong hệ thống thông tin, các lỗ hổng bảo mật và điểm yếu của hệ thống thông tin (HTTT), các dạng tấn công và phần mềm độc hại, phương pháp mã hóa và giải mã dữ liệu.

- CO 2: Có kiến thức về các kỹ thuật, phương pháp, qui tắc sử dụng trong phát hiện phòng chống xâm nhập, phương pháp đảm bảo an toàn thông tin, chính sách và pháp luật về an toàn thông tin.

*2.2.2. Về kỹ năng*

- CO 3: Có thể thiết lập được các cách phòng chống cho dữ liệu, máy tính.

- CO 4: Có kỹ năng thuyết trình, hoạt động nhóm

*2.2.3. Về năng lực tự chủ và trách nhiệm*

- CO 5: Tự học và phát triển kỹ năng phù hợp để có thể tham gia vào các dự án về an toàn thông tin

**3. Chuẩn đầu ra của học phần (CLOs)**

**Bảng 1. Chuẩn đầu ra (CLOs) của học phần**

Khi học xong học phần, SV có khả năng:

| **Ký hiệu** | **Chuẩn đầu ra học phần (CLOs)** | **Hỗ trợ cho**  **mục tiêu** |
| --- | --- | --- |
| CLO1 | Trình bày được khái niệm, đặc trưng, nguyên nhân và hiện trạng về tình hình an toàn thông tin hiện nay | CO1, CO3, CO4 |
| CLO2 | Trình bày được đặc trưng, ưu nhược điểm, các hoạt động cơ bản của lỗ hổng bảo mật và điểm yếu HTTT | CO1, CO4, CO5 |
| CLO3 | Trình bày được khái niệm, hình thức, cơ chế, nguyên nhân của các dạng tấn công và phần mềm độc hại. | CO1, CO4, CO5 |
| CLO4 | Trình bày được đặc trưng, ưu nhược điểm, các hoạt động cơ bản của phương pháp mã hóa và giải mã dữ liệu. | CO1, CO3, CO4, CO5 |
| CLO5 | Nêu được các đặc điểm phù hợp và chưa chưa phù hợp của hệ thống phát hiện tấn công và phòng chống xâm nhập | CO2, CO3, CO4, CO5 |
| CLO6 | Trình bày được các chính sách về an toàn thông tin. | CO2, CO3, CO4, CO5 |

**4. Mối liên hệ giữa CĐR HP(CLO) với CĐR CTĐT (PLO)**

Mức độ đóng góp, hỗ trợ của CLO đối với PLO được xác định cụ thể như sau:

*I (Introduced) – CLO có hỗ trợ đạt được PLO và ở mức giới thiệu/bắt đầu*

*R (Reinforced) – CLO có hỗ trợ đạt được PLO và ở mức nâng cao hơn mức bắt đầu, có nhiều cơ hội được thực hành, thí nghiệm, thực tế,…*

*M (Mastery) – CLO có hỗ trợ cao đạt được PLO và ở mức thuần thục/thông hiểu*

*A (Assessed) – Học phần quan trọng (hỗ trợ tối đa việc đạt được PLO) cần được thu thập minh chứng để đánh giá CĐR CTĐT.*

**Bảng 2. Mối liên hệ giữa CLO với PLO**

| **PLO** | (1) | (2 | (3) | (4) | (5) | (6) | (7) | (8) | (9) | (10) | (11) | (12) |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| CLO1 |  | I | R |  |  |  |  |  |  | I | I | I |
| CLO2 |  |  | R |  |  |  |  | I |  | R | I | I |
| CLO3 |  |  | R |  |  |  |  | R |  |  | R | I |
| CLO4 |  | R | I |  |  |  |  |  |  |  | I |  |
| CLO5 |  |  | I |  |  |  |  | I |  | R | R |  |
| CLO6 |  |  | R |  |  |  |  |  |  |  | R |  |
| Tổng hợp học phần |  | R | R |  |  |  |  | R |  | R | R | I |

**5. Học liệu[[2]](#endnote-2)**

***5.1. Tài liệu chính***

[1]. Phan Đình Diệu, (2004), *Lý thuyết mật mã và an toàn thông tin*, NXB Đại học Quốc gia Hà Nội.

***5.2. Tài liệu tham khảo***

[1]. Lê Quang Minh, (2015), *Bài giảng Nhập môn an toàn thông tin*, Đại học Quốc gia Hà Nội.

[2]. Trần Thị Kim Chi, (2015), *Bài giảng Nhập môn an toàn thông tin*, Đại học Công nghiệp TP.Hồ Chí Minh.

[3]. Đỗ Xuân Chợ, (2016), *Bài giảng mật mã học cơ sở*, Học viện Công nghệ bưu chính viễn thông.

[4]. TS.Nguyễn Khang Văn, (2014), *Cơ sở an toàn thông tin*, Đại học Bách Khoa Hà Nội.

[5]. Hoàng Xuân Dậu, (2008), *Bài giảng an toàn bảo mật hệ thống thông tin*, Học viện Công nghệ bưu chính viễn thông.

[6]. Trịnh Nhật Tiến, (2007), *Bài giảng An ninh dữ liệu*, NXB Đại học Quốc gia Hà Nội.

**6. Cấu trúc học phần**

- Tổng số tiết trên lớp: 3 tiết;

- Tổng số tuần học: 15 tuần;

- Phân bố: 3 tiết/ buổi x 1 buổi/ tuần = 15 buổi;

- Kiểm tra, đánh giá:`

+ Đánh giá chuyên cần: Tất cả các buổi học;

+ Kiểm tra định kì: 2 bài;

+ Thi kết thúc học phần: 1 bài

**7. Kế hoạch dạy học**

**Bảng 3. Kế hoạch dạy học[[3]](#endnote-3)**

| **Tuần**  **Buổi** | **Nội dung dạy học** | **Số tiết** | **CĐR**  **của bài học** | **Hướng tới**  **CLOs** | **Hoạt động**  **dạy - học** |
| --- | --- | --- | --- | --- | --- |
| 1 | **CHƯƠNG 1: TỔNG QUAN VỀ ATTT**  **1.1. Các khái niệm cơ bản**  **1.2. Các nguyên tắc nền tảng của an toàn thông tin**  1.2.1. Tính bí mật (Confidentiality)  1.2.2. Tính toàn vẹn (Integrity)1.2.3. Tính sẵn sàng (Availability)  1.2.4. Tính chống thoái thác (Non-repudiation)  **1.3. Các loại hình tấn công và nguy cơ mất ATTT**  1.3.1. Các khái niệm tấn công  1.3.2. Một số kỹ thuật tấn công mạng  1.3.3. Xu hướng tấn công HTTT  1.3.4. Các nguy cơ mất ATTT | 3 | Trình bày và giải thích được các khái niệm cơ bản của ATTT.  Trình bày được tính bí mật của HTTT  Trình bày được tính toàn vẹn của HTTT  Trình bày được tính sẵn sàng của HTTT  Trình bày được tính chống thoái thác của HTTT  Liệt kê và phân tích được các đặc điểm cơ bản về nguy cơ mất ATTT hiện nay. | CLO1 | GV trình bày, hướng dẫn  SV lắng nghe, thực hiện |
| 2 | **1.4. Giải pháp đảm bảo an toàn thông tin**  **1.5. Các bài toán an toàn thông tin cơ bản**  1.5.1. Bài toán bảo mật: mã hóa và phong bì số  1.5.2. Chữ ký số (Digital signature):  1.5.3. Bài toán chứng thực và toàn vẹn: chữ ký số và mã chứng thực  **Câu hỏi và bài tập chương 1** | 3 | Liệt kê được các giải pháp đảm bảo ATTT  Vận dụng kiến thức đã học để giải các bài toán về mã hóa và phong bì số, chữ ký số, bài toán chứng thực và toàn vẹn. | CLO1 | GV trình bày, hướng dẫn  SV lắng nghe, thực hiện |
| 3 | **CHƯƠNG 2: CÁC LỖ HỔNG BẢO MẬT VÀ ĐIỂM YẾU HTTT**  **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**  2.2.1. Lỗi tràn bộ đệm  2.2.2. Lỗi không kiểm tra đầu vào  2.2.3. Các vấn đề với điều khiển truy nhập  2.2.4. Các điểm yếu trong xác thực, trao quyền  2.2.5. Các điểm yếu trong các hệ mật mã  2.2.6. Các lỗ hổng bảo mật khác | 3 | Trình bày và giải thích được các lỗ hổng bảo mật và các điểm yếu của hệ thống  Trình bày và phân tích được dạng lỗ hổng tràn bộ đệm | CLO2 | GV trình bày, hướng dẫn  SV lắng nghe, thực hiện |
| 4 | **2.3. Quản lý, khắc phục các lỗ hổng bảo mật và tăng cường khả năng đề kháng cho hệ thống**  2.3.1. Nguyên tắc chung  2.3.2. Các biện pháp cụ thể  **2.4. Giới thiệu một số công cụ rà quét điểm yếu và lỗ hổng bảo mật**  2.4.1. Công cụ rà quét lỗ hổng bảo mật hệ thống  2.4.2. Công cụ rà quét lỗ hổng ứng dụng web  **Câu hỏi và bài tập chương 2** | 3 | Liệt kê được các đặc điểm cơ bản về quản lý, khắc phục các lỗ hổng bảo mật và tăng cường khả năng đề kháng cho hệ thống.  Liệt kê được một số công cụ rà quét lỗ hổng bảo mật có nhiều ưu điểm nhất hiện nay | CLO2 | GV trình bày, hướng dẫn  SV lắng nghe, thực hiện |
| 5 | **CHƯƠNG 3: CÁC DẠNG TẤN CÔNG VÀ CÁC PHẦN MỀM ĐỘC HẠI**  **3.1. Khái quát về mối đe dọa và tấn công**  3.1.1. Mối đe dọa  3.1.2. Tấn công  **3.2. Các công cụ hỗ trợ tấn công**  3.2.1. Công cụ quét cổng dịch vụ  3.2.2. Công cụ nghe lén  3.2.3. Công cụ ghi phím gõ | 3 | Trình bày được các khái niệm về mối đe dọa và tấn công  Trình bày và giải thích được các công cụ tấn công vào hệ thống thông tin bao gồm: Công cụ quét cổng dịch vụ, công cụ nghe lén, công cụ ghi phím gõ | CLO3 | GV trình bày, hướng dẫn  SV lắng nghe, thực hiện |
| 6 | **3.3. Các dạng tấn công thường gặp**  3.3.1. Tấn công vào mật khẩu  3.3.2. Tấn công bằng mã độc  3.3.3. Tấn công từ chối dịch vụ  3.3.4. Tấn công giả mạo địa chỉ  3.3.5. Tấn công nghe lén  3.3.6. Tấn công kiểu người đứng giữa  3.3.7. Tấn công bằng bom thư và thư rác  3.3.8. Tấn công sử dụng các kỹ thuật xã hội  3.3.9. Tấn công pharming | 3 | Trình bày và nêu được các ưu nhược điểm của tấn công vào mật khẩu, tấn công bằng mã độc, tấn công từ chối dịch vụ, tấn công giả mạo địa chỉ, tấn công nghe lén, tấn công kiểu người đứng giữa, tấn công bằng bom thư và thư rác, tấn công sử dụng các kỹ thuật xã hội, tấn công pharming | CLO3 | GV trình bày, hướng dẫn  SV lắng nghe, thực hiện |
| 7 | **3.4. Mã độc**  3.4.1. Giới thiệu Malware  3.4.2. Phân loại Malware  **Câu hỏi và bài tập chương 3** | 3 | Trình bày và giải thích được khái niệm, phân loại Malware | CLO3 | GV trình bày, hướng dẫn  SV lắng nghe, thực hiện |
| 8 | **CHƯƠNG 4: PHƯƠNG PHÁP MÃ HÓA VÀ GIẢI MÃ DỮ LIỆU**  **4.1. Mã hóa**  4.1.1. Một số khái niệm về mã hóa  4.1.2. Sơ đồ mã hóa  4.1.3. Mã hóa cổ điển | 3 | Trình bày được khái niệm, phân loại mã hóa.  Trình bày được nguyên lý mã hóa và giải mã. | CLO4 | GV trình bày, hướng dẫn  SV lắng nghe, thực hiện |
| 9 | **4.2. Hàm băm và ứng dụng**  4.2.1. Định nghĩa  4.2.2.Một số hàm băm thông dụng  4.2.3. Ứng dụng của hàm băm  4.2.4. Tấn công hàm băm | 3 | Trình bày được khái niệm, ứng dụng, tấn công hàm băm | CLO4 | GV trình bày, hướng dẫn  SV lắng nghe, thực hiện |
| 10 | **4.3. Mã chứng thực thông điệp**  4.3.1. Khái niệm  4.3.2. Mục tiêu của xác thực thông điệp:  4.3.3. Mã hóa thông điệp: (Sử dụng mã hóa khóa bí mật, mã hóa khóa công khai)  4.3.4. Mã chứng thực thông điệp  **4.4. Chữ ký điện tử**  4.4.1. Khái niệm chữ ký điện tử  4.4.2. Một số loại chữ ký số | 3 | Trình bày được khái niệm, mục tiêu của mã chứng thực thông điệp  Trình bày được khái niệm, phân loại chữ ký số | CLO4 | GV trình bày, hướng dẫn  SV lắng nghe, thực hiện |
| 11 | **4.5. Kiến trúc khóa công khai**  4.5.1. Mô hình kiến trúc khóa công khai  4.5.2. Các chức năng quản trị PKIX  4.5.3. Phân phối khóa (Key Distribution)  4.5.4. Thẻ chứng thực X.509  4.5.5. Kerberos  **4.6. Chứng thực thực thể**  4.6.1. Khái niệm  4.6.2. Fixed password:  4.6.3. One-time Password  4.6.4. Dùng Sysmetric-Key Cipher  4.6.5. Using Keyed-Has Functions  4.6.6. Sử dụng mã hóa khóa đối xứng (Asymmetric-Key Cipher)  4.6.7. ZERO-KNOWLEDGE  **Câu hỏi và bài tập chương 4** | 3 | Trình bày được khái niệm, mô hình kiến trúc khóa công khai  Trình bày được khái niệm, các ứng dụng của chứng thực thực thể. | CLO4 | GV trình bày, hướng dẫn  SV lắng nghe, thực hiện |
| 12 | **CHƯƠNG 5 : HỆ THỐNG PHÁT HIỆN VÀ PHÒNG CHỐNG XÂM NHẬP**  **5.1. Tường lửa**  5.1.1. Giới thiệu tường lửa  5.1.2. Phân loại tường lửa  5.1.3. Các kỹ thuật kiểm soát truy nhập  5.1.4. Các hạn chế của tường lửa  **5.2. Hệ thống Proxy**  5.2.1. Proxy server là gì?  5.2.2. Mục đích của Proxy server  5.2.3. Phân loại Proxy server  5.2.4. Summary | 3 | Trình bày được khái niệm, phân loại, các kỹ thuật kiểm soát tường lửa.  Trình bày được khái niệm, mục đích, phân loại, cơ chế hoạt động Proxy server | CLO5 | GV trình bày, hướng dẫn  SV lắng nghe, thực hiện |
| 13 | **5.3. IDS và IPS?**  5.3.1. Tổng quan về IDS và IPS  5.3.2. Thành phần chính về IDS và IPS  5.3.3. Phân loại IDS và IPS  5.3.4. Các kỹ thuật phát hiện xâm nhập  5.3.5. Snort  **5.4. Một số giao thức bảo mật thông dụng**  5.4.1. Các giao thức bảo mật E-mail  5.4.2. Các giao thức bảo mật mạng  **Câu hỏi và bài tập chương 5** | 3 | Trình bày được các đặc điểm tổng quan cơ bản của IDS/IPS.  Trình bày được một số giao thức bảo mật thông tin | CLO5 | GV trình bày, hướng dẫn  SV lắng nghe, thực hiện |
| 14 | **CHƯƠNG 6. CHÍNH SÁCH VÀ PHÁP LUẬT AN TOÀN THÔNG TIN**  **6.1. Giới thiệu chung**  6.1.1. Khái quát về quản lý an toàn thông tin  6.1.2. Đánh giá rủi ro an toàn thông tin  6.1.3. Phân tích chi tiết rủi ro an toàn thông tin  6.1.4. Thực thi quản lý an toàn thông tin  6.1.5. Tin tặc, tội phạm kỹ thuật  6.1.6. Một số tội phạm tin học liên quan đến Internet  **6.2. Pháp luật và chính sách an toàn thông tin**  6.2.1. Giới thiệu về pháp luật và chính sách an toàn thông tin  6.2.2. Vấn đề sở hữu trí tuệ và bản quyền  6.2.3. Luật quốc tế về an toàn thông tin  6.2.4. Luật Việt Nam về an toàn thông tin | 3 | Nêu được tầm quan trọng của pháp luật ATTT.  Trình bày và giải thích được các Luật Việt Nam về ATTT | CLO6 | GV trình bày, hướng dẫn  SV lắng nghe, thực hiện |
| 15 | **6.3. Vấn đề đạo đức an toàn thông tin**  6.3.1. Sự cần thiết của đạo đức an toàn thông tin  6.3.2. Một số bộ quy tắc ứng xử trong CNTT và ATTT  6.3.3. Một số vấn đề khác  **6.4. Giới thiệu bộ chuẩn an toàn thông tin ISO 27000**  **Câu hỏi và bài tập chương 6** | 3 | Trình bày và giải thích được các vấn đề đạo đức trong ATTT.  Trình bày được bộ chuẩn ATTT ISO 27000.  Vận dụng được luật ATTT trong công tác thực tế. | CLO6 | GV trình bày, hướng dẫn  SV lắng nghe, thực hiện |

(\*) Giới thiệu học phần: Vị trí, vai trò của học phần trong CTĐT của ngành; CO, CLO, nội dung học phần, các hình thức, trọng số, tiêu chí, biểu điểm các bài kiểm tra, …

**8. Đánh giá học phần**

***8.1. Phương pháp, hình thức kiểm tra - đánh giá***

**Bảng 4. Kiểm tra - đánh giá**

| **Thành phần, tên bài đánh giá** | **Trọng số** | **Nội dung đánh giá** | **Trọng số**  **con** | **Rubric**  **(đánh dấu x nếu có)** | **Hướng tới**  **đánh giá CLOs** | **Cách thức đánh giá** |
| --- | --- | --- | --- | --- | --- | --- |
| A1  Đánh giá chuyên cần | 10% | Ý thức tham gia học tập |  |  |  | Theo dõi và đánh giá cả quá trình học tập. |
| A2  Đánh giá định kỳ | 30% | Kiến thức về Các loại hình tấn công và nguy cơ mất ATTT hiện nay.  Giải pháp đảm bảo An toàn thông tin.  Tổng quan về lỗ hổng bảo mật và các điểm yếu hệ thống  Quản lý, khắc phục các lỗ hổng bảo mật và tăng cường khả năng đề kháng cho hệ thống  Giới thiệu một số công cụ rà quét lỗ hổng bảo mật. | 50% |  | CLO1CLO2 CLO3  CLO4 | SV làm bài viết trên lớp, GV thu bài về chấm điểm |
| Kiến thức về Một số kỹ thuật tấn công HTTT  Phương pháp mã hóa và giải mã dữ liệu.  Hệ thống phát hiện và phòng chống xâm nhập  Chính sách và pháp luật ATTT | 50% |  | CLO5 CLO6 | SV làm bài viết trên lớp, GV thu bài về chấm điểm |
| A3  Đánh giá cuối kỳ | 60% | Kiến thức về các loại hình tấn công và nguy cơ mất ATTT hiện nay.  Giải pháp đảm bảo An toàn thông tin.  Tổng quan về lỗ hổng bảo mật và các điểm yếu hệ thống  Quản lý, khắc phục các lỗ hổng bảo mật và tăng cường khả năng đề kháng cho hệ thống  Giới thiệu một số công cụ rà quét lỗ hổng bảo mật.  Kiến thức về Một số kỹ thuật tấn công HTTT  Phương pháp mã hóa và giải mã dữ liệu.  Hệ thống phát hiện và phòng chống xâm nhập  Chính sách và pháp luật ATTT |  |  | CLO1CLO2  CLO3CLO4CLO5CLO6 | Sinh viên làm bài thi lý thuyết theo tổ chức của phòng Khảo thí, giáo viên chấm điểm. |

***8.2. Tiêu chí đánh giá***

*8.2.1. Đánh giá chuyên cần*

- Đi học đầy đủ: 6 điểm (60%, nghỉ 3 tiết học không lý do trừ 1 điểm)

- Hoàn thành đúng hạn các yêu cầu của giảng viên: 2 điểm (20%)

- Tích cực phát biểu, thảo luận trên lớp: 1 điểm (10%)

- Tự học, chủ động tìm tòi kiến thức: 1 điểm (10%)

*8.2.2. Kiểm tra định kỳ*

\* Bài kiểm tra 1:

- Nội dung:

+ Các loại hình tấn công và nguy cơ mất ATTT hiện nay.

+ Giải pháp đảm bảo An toàn thông tin.

+ Tổng quan về lỗ hổng bảo mật và các điểm yếu hệ thống

+ Quản lý, khắc phục các lỗ hổng bảo mật và tăng cường khả năng đề kháng cho hệ thống

+ Giới thiệu một số công cụ rà quét lỗ hổng bảo mật.

- Thời gian: 50 phút

- Hình thức: Kiểm tra viết

| **STT** | **Nội dung** | **Tiêu chí đánh giá** |  | **Điểm** |
| --- | --- | --- | --- | --- |
| 1 | + Các loại hình tấn công và nguy cơ mất ATTT hiện nay.  + Giải pháp đảm bảo An toàn thông tin.  + Tổng quan về lỗ hổng bảo mật và các điểm yếu hệ thống  + Quản lý, khắc phục các lỗ hổng bảo mật và tăng cường khả năng đề kháng cho hệ thống  + Giới thiệu một số công cụ rà quét lỗ hổng bảo mật. | Đúng kiến thức, đủ yêu cầu | | 5 |
| 2 | Nêu và phân tích được một số ứng dụng thực tế đang bị mất an toàn thông tin | Đúng kiến thức, đủ yêu cầu | | 5 |
| **Tổng điểm** | | | | **10** |

\* Bài kiểm tra 2:

- Nội dung:

+ Một số kỹ thuật tấn công HTTT

+ Phương pháp mã hóa và giải mã dữ liệu.

+ Hệ thống phát hiện và phòng chống xâm nhập

+ Chính sách và pháp luật ATTT

- Thời gian: 50 phút

- Hình thức: Kiểm tra viết

**Bảng 5. Tiêu chí, biểu điểm đánh giá bài kiểm tra định kì**

| **STT** | **Nội dung** | **Tiêu chí đánh giá** |  | **Điểm** |
| --- | --- | --- | --- | --- |
| 1 | Kiến thức về Một số kỹ thuật tấn công HTTT  Phương pháp mã hóa và giải mã dữ liệu.  Hệ thống phát hiện và phòng chống xâm nhập  Chính sách và pháp luật ATTT | Đúng kiến thức, đủ yêu cầu | | 5 |
| 2 | Nêu và phân tích được một số kỹ thuật tấn công HTTT hiện nay. | Đúng kiến thức, đủ yêu cầu | | 5 |
| **Tổng điểm** | | | | **10** |

*8.2.3. Thi kết thúc học phần*

- Nội dung: Kiến thức về quá trình phát triển phần mềm

- Hình thức: Thi viết

- Thời gian: 90 phút

**Bảng 6. Tiêu chí, biểu điểm đánh giá bài thi kết thúc học phần**

| **STT** | **Nội dung** | **Tiêu chí đánh giá** |  | **Điểm** |
| --- | --- | --- | --- | --- |
| 1 | Các loại hình tấn công và nguy cơ mất ATTT hiện nay.  Giải pháp đảm bảo An toàn thông tin.  Tổng quan về lỗ hổng bảo mật và các điểm yếu hệ thống  Quản lý, khắc phục các lỗ hổng bảo mật và tăng cường khả năng đề kháng cho hệ thống  Giới thiệu một số công cụ rà quét lỗ hổng bảo mật. | Đúng kiến thức, đủ yêu cầu | | 5 |
| 2 | Một số kỹ thuật tấn công HTTT  Phương pháp mã hóa và giải mã dữ liệu.  Hệ thống phát hiện và phòng chống xâm nhập  Chính sách và pháp luật ATTT. | Đúng kiến thức, đủ yêu cầu | | 5 |
| **Tổng điểm** | | | | **10** |

*Quảng Ninh, ngày 20 tháng 7 năm 2020*

|  |  |  |  |
| --- | --- | --- | --- |
| **Hiệu trưởng** | **Trưởng khoa**  **Lương Khắc Định** | **Trưởng bộ môn** | **Người biên soạn**  **Trịnh Thị Vân** |

1. Mục tiêu chung của học phần bắt đầu bằng: Sau khi học xong học phần, sinh viên ..... [↑](#endnote-ref-1)
2. Học liệu có thể là học liệu tiếng Việt hoặc tiếng nước ngoài, ghi theo trật tự: Tên tác giả (năm xuất bản), tên tài liệu, nhà xuất bản, nơi xuất bản]. [↑](#endnote-ref-2)
3. Một số lưu ý khi xây dựng bảng 3 thuộc mục 7. Kế hoạch dạy học:

   1. Cần xác định rõ tuần thứ bao nhiêu, buổi thứ bao nhiêu sẽ có bài kiểm tra định kì.

   2. Nếu buổi học nào có yêu cầu đặc biệt về cơ sở vật chất phục vụ dạy học (phương tiện hỗ trợ, phòng học, không gian học tập/ thực hành/ dã ngoại, ...) thì GV bổ sung xuống phần chú ý ở sau bảng 3. [↑](#endnote-ref-3)